RSAC 2025 Conference

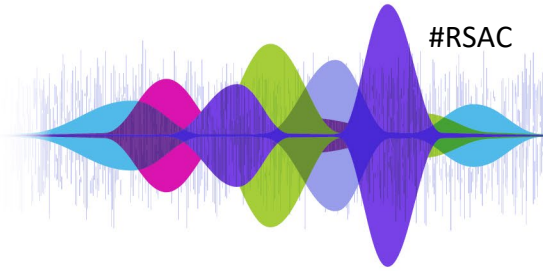
Many Voices.
One Community.

SESSION ID: PDP-W01

Every Move You Make
Every App You Play
I'll Be Watching You

Mattia Epifani

Certified Instructor @ SANS Institute
CEO @ REALITY NET
https://it.linkedin.com/in/mattiaepifani

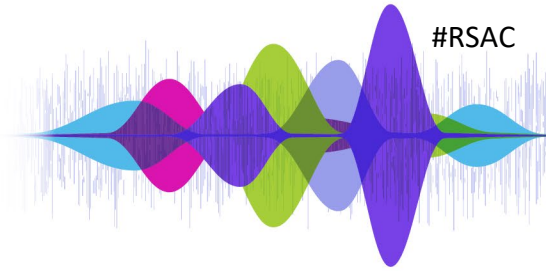


Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.



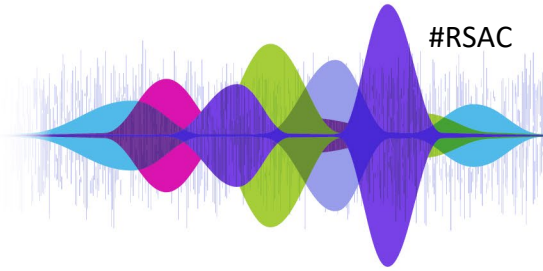
Agenda

- Mobile Forensics
- Data-at-rest encryption on mobile devices
- Data extraction from Mobile Devices
- Building the user “pattern of life”
- Most relevant artifacts on Android and iOS devices
- Key takeaways

Mobile Forensics and encryption

- In the pre-smartphone era, mobile devices **lacked robust encryption mechanisms**, leaving users' data vulnerable to unauthorized access
- Today, encryption has become **a standard feature on both Android and iOS devices**
- Modern smartphones use **various encryption techniques** to protect sensitive data stored on the device

Android Encryption (simplified)

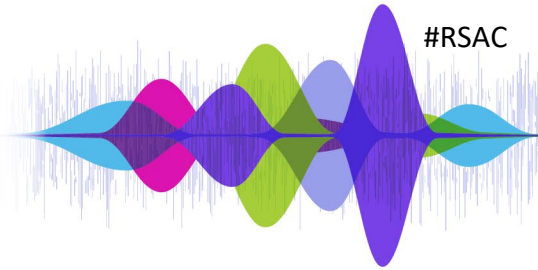


- https://source.android.com/docs/security/features/encryption
- Encryption is the process of **encoding all user data** on an Android device using **symmetric encryption keys**
- Once a device is encrypted, **all user-created data is automatically encrypted before committing it to disk** and **all reads automatically decrypt data before returning it to the calling process**
- Android has two methods for device encryption:
  - **Full-disk encryption** (**FDE**) — Android 5 to Android 10 (up to 12 if upgraded)
  - **File-based encryption** (**FBE**) — Android 10 and above

Android FBE

- https://source.android.com/docs/security/features/encryption/file-based
- File-based encryption allows **different files to be encrypted with different keys that can be unlocked independently**
- File-based encryption enables a new feature called **Direct Boot,** that allows encrypted devices to boot straight to the lock screen
- An FBE device has two storage locations available to applications:
  - **Credential Encrypted (CE)**: file is only available after the user has unlocked the device
  - **Device Encrypted (DE)**: file is available both during Direct Boot mode and after the user has unlocked the device

Android FBE and Mobile Forensics

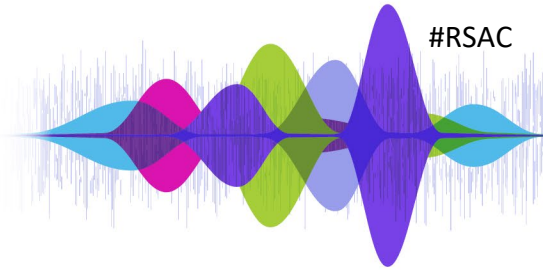


- Old “physical” methods are not viable (JTAG, Chip Off, ISP)
- Each file has its own encryption key, so it impossible to recover deleted files: the **encryption key is wiped when a file is deleted**
- **Suitable exploits can be used to access device-encrypted files without knowing the passcode**
- User passcode is tied to credential-encrypted files

Android AFU vs BFU

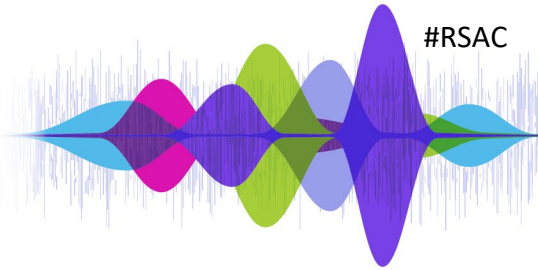
- **BFU = Before First Unlock**
- When a device is restarted, **only device-encrypted files are decrypted**
- **AFU = After First Unlock**
- As soon as the user has entered the passcode for the first time, **all files are decrypted**
- **With a suitable exploit, you can read encryption keys from the RAM of a device in AFU state**
- **It is not necessary to crack the passcode!**

iOS Encryption (simplified)



- https://help.apple.com/pdf/security/en_US/apple-platform-security-guide.pdf
- Apple uses a technology called **Data Protection** to protect data stored in flash storage on the devices that feature an Apple SoC (iPhone, iPad, Apple Watch and Apple TV)
- With Data Protection, a device can respond to common events such as incoming phone calls while at the same time providing a high level of encryption for user data
- Certain system apps (such as Messages, Mail, Calendar, Contacts, Photos) and Health data values use Data Protection by default
- Third-party apps receive this protection automatically

iOS Encryption (simplified)



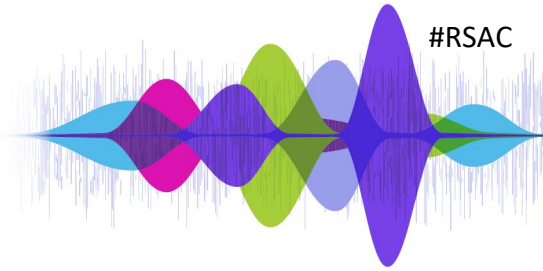
- Data Protection is implemented by constructing and managing **a hierarchy of keys** and **builds on the hardware encryption technologies built into Apple devices**
- Data Protection is controlled **on a per-file basis** by **assigning each file to a class**
- Accessibility is determined according to **whether the class keys have been unlocked**

iOS Encryption (simplified)

- When a new file is created on devices supporting Data Protection, **it's assigned a class by the app that creates it**
- Each class uses different policies to determine when the data is accessible

Class	Protection type
Class A: Complete Protection	NSFileProtectionComplete
Class B: Protected Unless Open	NSFileProtectionCompleteUnlessOpen
Class C: Protected Until First User Authentication *Note:* macOS uses a volume key to recreate FileVault protection characteristics.	NSFileProtectionCompleteUntilFirstUserAuthentication
Class D: No Protection *Note:* Not supported in macOS.	NSFileProtectionNone

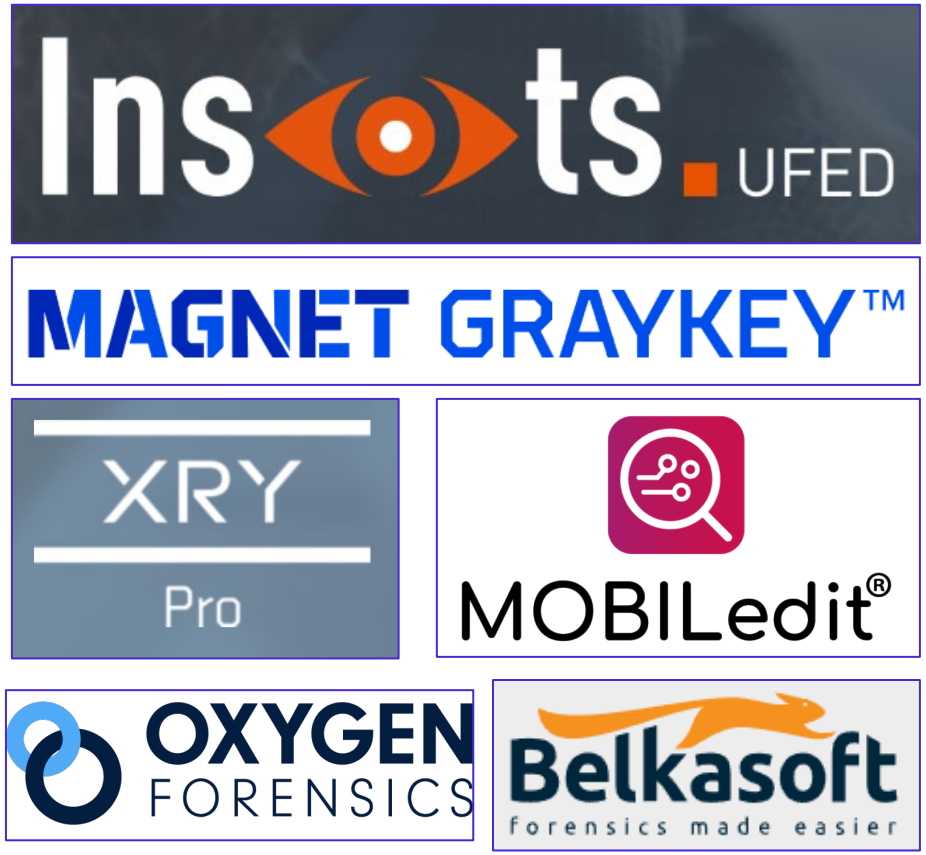
iOS AFU vs BFU



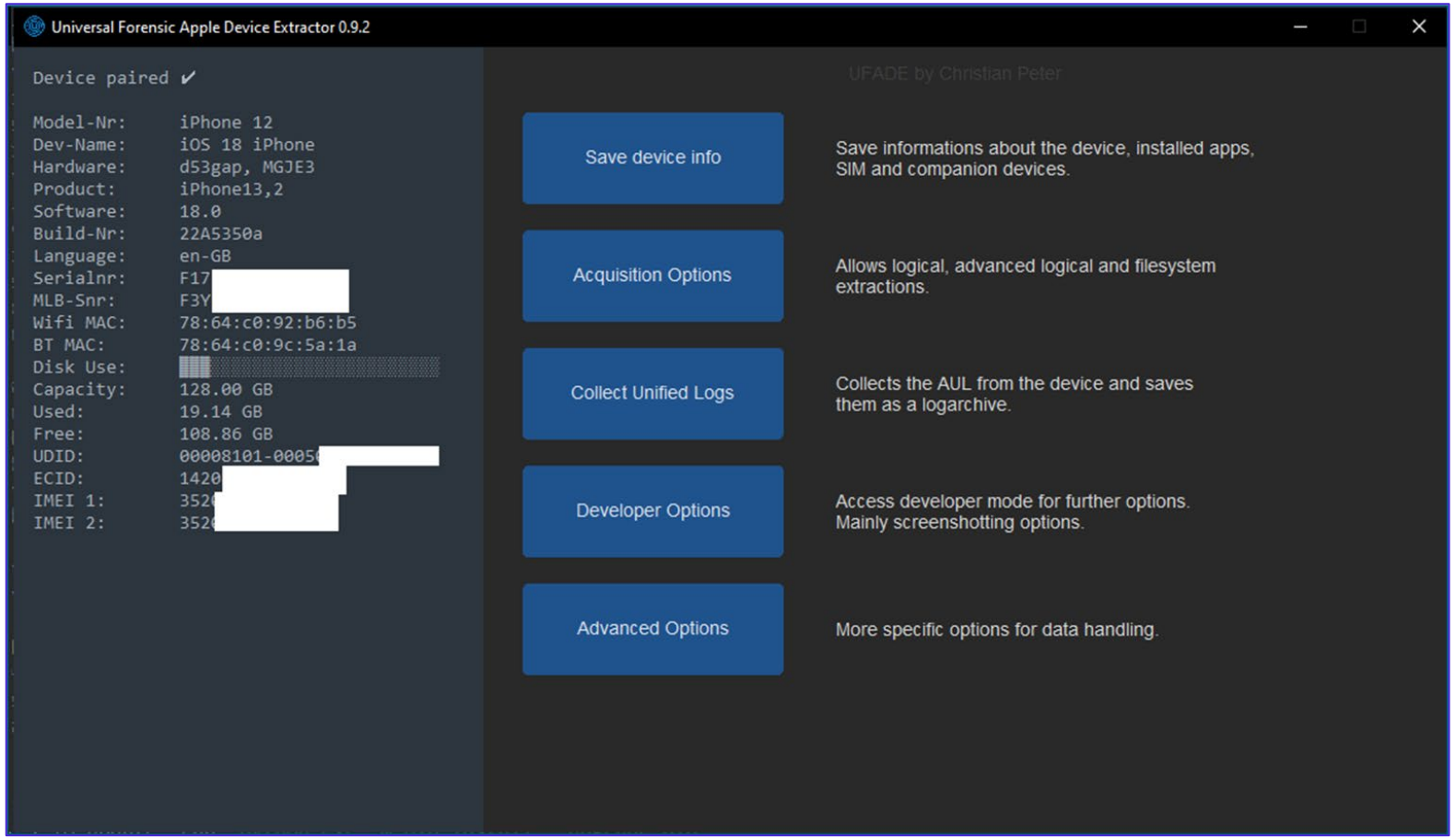
- **BFU = Before First Unlock**
- When a device is restarted, **only Class D files are decrypted**
- **AFU = After First Unlock**
- As soon as the user has entered the passcode for the first time, **all files in Class C are decrypted**
- With a suitable exploit, you can read encryption keys for Class C and Class D files from the RAM of a device in AFU state: **it is not necessary to crack the passcode**
- **To decrypt files in Class A and B you need to know/crack the passcode**

Mobile Forensics acquisition

- Mobile devices restrict access to only some communication protocols
  - On Android devices, ADB and MTP
  - On iOS devices, iTunes Backup and AFC
- To get a Full File System extraction, **you need to get (temporary) root access**
- Limited support from open/free tools
- In most cases you need a commercial tool

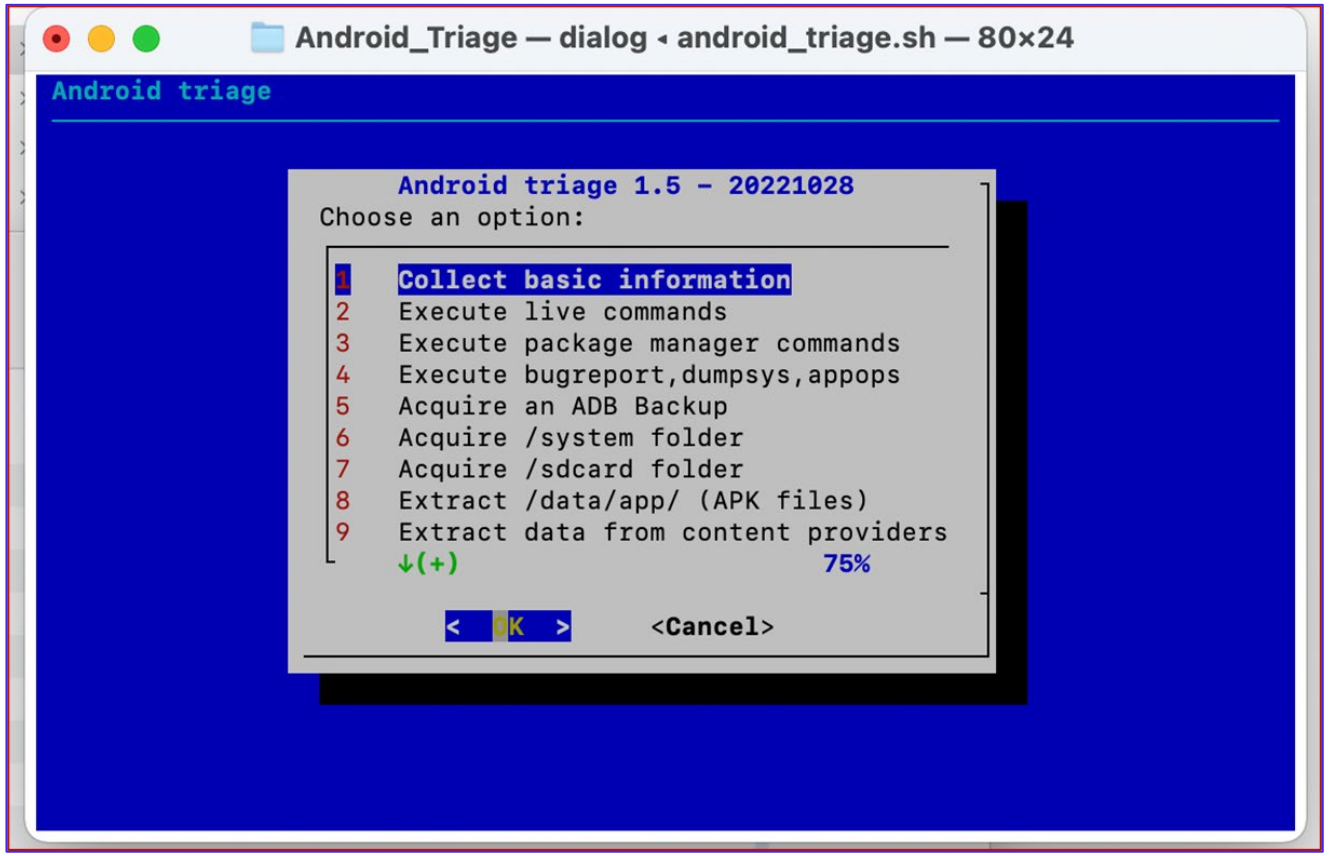


UFADE (Windows/Mac)



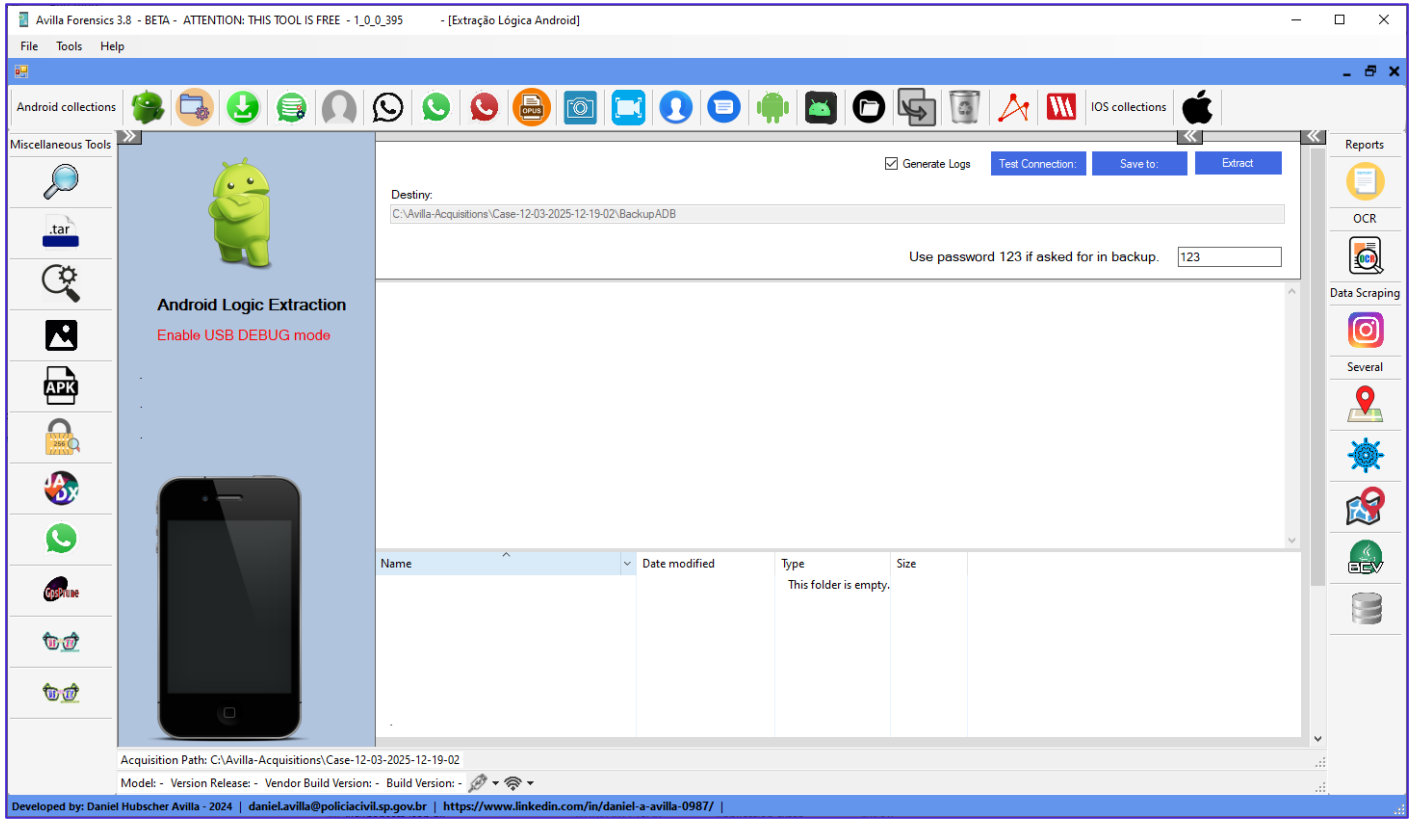
https://github.com/prosch88/UFADE

Android Triage (Mac/Linux)


Android_Triage — dialog ◂ android_triage.sh — 80×24
Android triage
Android triage 1.5 - 20221028
Choose an option:
1 Collect basic information
2 Execute live commands
3 Execute package manager commands
4 Execute bugreport,dumpsys,appops
5 Acquire an ADB Backup
6 Acquire /system folder
7 Acquire /sdcard folder
8 Extract /data/app/ (APK files)
9 Extract data from content providers
↓(+) 75%
< OK >
<Cancel>

https://github.com/RealityNet/android_triage

Avilla Forensics (Windows)



https://github.com/AvillaDaniel/AvillaForensics

Building the user Pattern of Life

- In most crimes, **locations** and **pattern of life** are analyzed
- Most devices record user activity to improve the user experience
- Both Android and iOS record various activities in common file formats
  - SQLite
  - LevelDB
  - XML/ABX
  - Plist
  - JSON

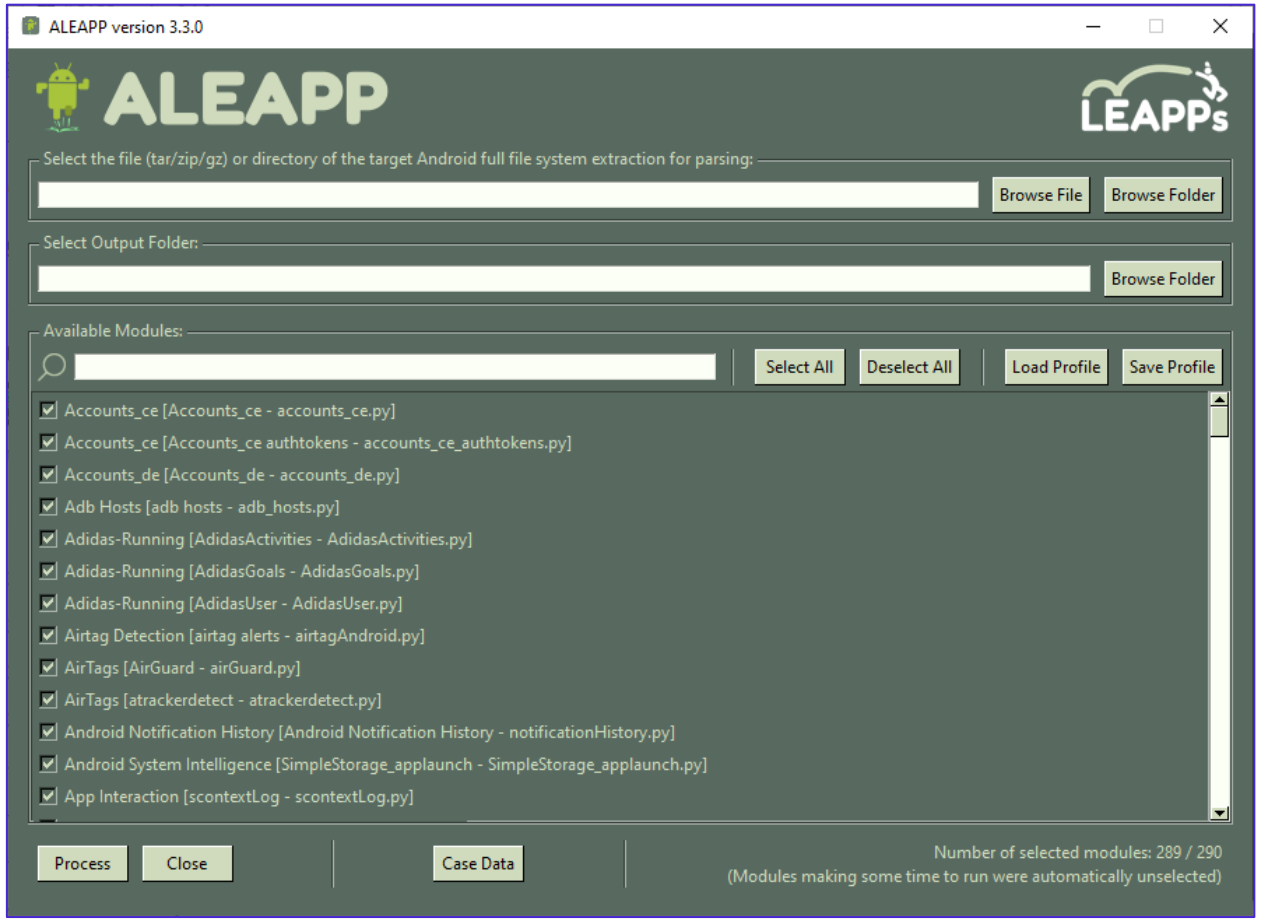
Building the user Pattern of Life

- Some of the most commonly analysed artifacts
  - Installed and uninstalled applications
  - User accounts
  - Network Connections
  - Application usage
  - Geolocation
  - Health
  - Application data

RSAC 2025 Conference

Android

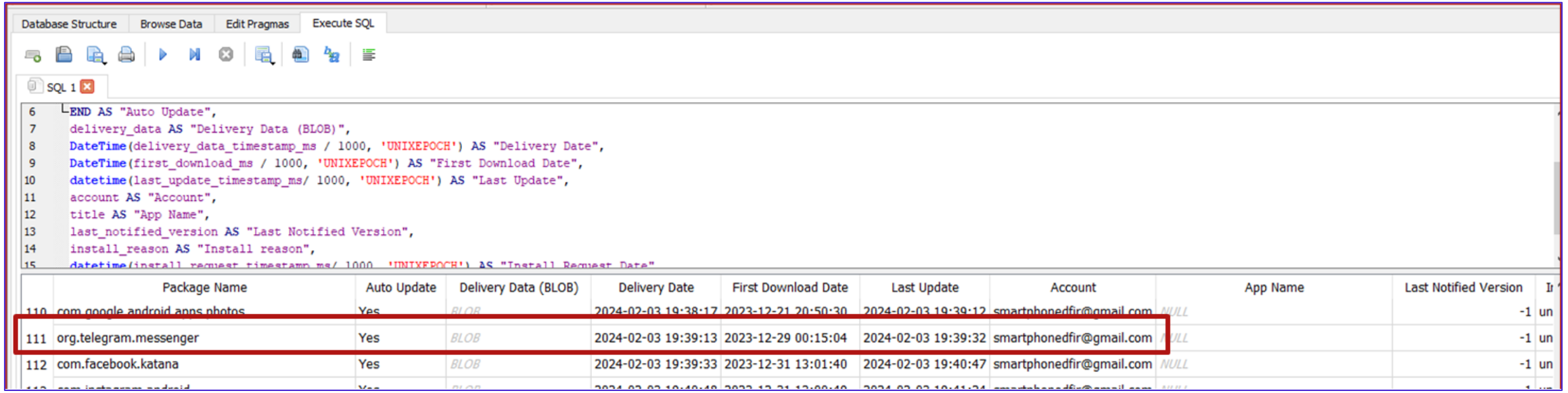
aLEAPP


ALEAPP version 3.3.0
ALEAPP
LEAPPs
Select the file (tar/zip/gz) or directory of the target Android full file system extraction for parsing:
Browse File
Browse Folder
Select Output Folder:
Browse Folder
Available Modules:
Select All
Deselect All
Load Profile
Save Profile
Accounts_ce [Accounts_ce - accounts_ce.py]
Accounts_ce [Accounts_ce authtokens - accounts_ce_authtokens.py]
Accounts_de [Accounts_de - accounts_de.py]
Adb Hosts [adb hosts - adb_hosts.py]
Adidas-Running [AdidasActivities - AdidasActivities.py]
Adidas-Running [AdidasGoals - AdidasGoals.py]
Adidas-Running [AdidasUser - AdidasUser.py]
Airtag Detection [airtag alerts - airtagAndroid.py]
AirTags [AirGuard - airGuard.py]
AirTags [atrackerdetect - atrackerdetect.py]
Android Notification History [Android Notification History - notificationHistory.py]
Android System Intelligence [SimpleStorage_applaunch - SimpleStorage_applaunch.py]
App Interaction [scontextLog - scontextLog.py]
Process
Close
Case Data
Number of selected modules: 289 / 290
(Modules making some time to run were automatically unselected)

https://github.com/abrignoni/ALEAPP

Installed and uninstalled applications

- **localappstate.db**
- Tracks applications installed on the device via the Google Play Store
- The information is **retained even after uninstalling the application**


Database Structure
Browse Data
Edit Pragmas
Execute SQL
SQL 1
END AS "Auto Update",
delivery_data AS "Delivery Data (BLOB)",
DateTime(delivery_data_timestamp_ms / 1000, 'UNIXEPOCH') AS "Delivery Date",
DateTime(first_download_ms / 1000, 'UNIXEPOCH') AS "First Download Date",
datetime(last_update_timestamp_ms/ 1000, 'UNIXEPOCH') AS "Last Update",
account AS "Account",
title AS "App Name",
last_notified_version AS "Last Notified Version",
install_reason AS "Install reason",
Package Name
Auto Update
Delivery Data (BLOB)
Delivery Date
First Download Date
Last Update
Account
App Name
Last Notified Version
110 com.google.android.apps.photos Yes 2024-02-03 19:38:17 2023-12-21 20:50:30 2024-02-03 19:39:12 smartphonedfir@gmail.com -1
111 org.telegram.messenger Yes 2024-02-03 19:39:13 2023-12-29 00:15:04 2024-02-03 19:39:32 smartphonedfir@gmail.com -1
112 com.facebook.katana Yes 2024-02-03 19:39:33 2023-12-31 13:01:40 2024-02-03 19:40:47 smartphonedfir@gmail.com -1

Installed and uninstalled applications

- **gass.db**
- Tracks applications regardless of how they were installed
- The information is **retained even after uninstalling the application**

	Package Name	Version Code	SHA-256
248	com.google.android.apps.scone	21828	5754f963ddbcac1d96637b69fbf16d928351cec2b97ee74ec54f8ef90536182e
249	com.google.android.apps.photos	48769065	ccebfeb93861358addb9925b60e2deafbdaadd4b8709f0da812f5a1bea729c9e
250	org.telegram.messenger	43552	b4bbb9986cf0aa903432b78fabff084d6698829c3558fe83748fc55cd7eaa3b4
251	com.facebook.katana	448814516	982bf08b3ac79a46c1eaaf995a33d0d8c085d453687ea047a088c2f7ecc23cce
252	com.instagram.android	371611289	4082ed99f6ede75ad889b25f5d5d1a31c294180ac0b9073bbd92ce5cf397ae04
253	com.google.android.apps.nbu.files	695143	c53d9bff30e9108154fc2996d4fc5cd84da1ca3a7228104b839f8911ea32b571
254	com.bereal.ft	1649	d2fbf9ff50cec762154e9b4f7ddc57f94bffa4d81a50801f07064bb368631790
255	com.google.android.dialer	15435008	e6b988378095c397f38511eda5b96c59e66bddefa3b4c789dfdcf1313fef6ca1
256	com.bskyb.skynews.android	491000123	6cbcf971c2c50ff7171373105b29f3a95c1800b93a11a3a9b3964a4d10661a41
257	com.google.ambient.streaming	10051700	308e5084c7d0fd3c341ede5e4a94ba9810498020d685518a15cf586c52da17da
258	com.google.android.marvin.talkback	60134389	34a93221d90c2239d04e9fd58702021c1432fe7c917899b1398701c3ca9f77f1
259	com.google.android.apps.subscriptions.red	491203	b016e53e66fcf77410ce340a1661507b716844f4b6deedcb233da49e48a02ccd
260	com.google.android.videos	439129267	eb14b3eb229eccde99d7b6ccd62a4fc5a09a34c6e3c77f0a0fe89b43dc88b250
261	org.thoughtcrime.securesms	137702	d502808100a795831cd23a94aa1aa916a98db15ddee69db756cd341e6c3013bd

User Accounts

- **accounts_de.db**
- Tracks user accounts
- File is device-encrypted → **not protected with user passcode**

	App	Account	Action	Action Time
1	com.google	smartphonedfir@gmail.com	action_account_add	2023-12-21 20:40:02
2	com.google	smartphonedfir@gmail.com	action_set_password	2023-12-21 20:40:02
3	com.whatsapp	WhatsApp	action_account_add	2023-12-29 01:16:42
4	org.telegram.messenger	6315479848	action_account_add	2023-12-29 01:17:31
5	org.thoughtcrime.securesms	Signal	action_account_add	2023-12-29 01:18:47
6	com.duolingo	Duolingo	action_account_add	2023-12-30 10:49:37
7	com.reddit.account	Reddit for Android	action_account_add	2023-12-31 09:34:21
8	com.reddit.account	Tight-Entertainer885	action_account_add	2023-12-31 09:34:32
9	com.dropbox.android.multiaccount	smartphonedfir@gmail.com	action_account_add	2023-12-31 09:36:28
10	com.facebook.messenger	Messenger	action_account_add	2023-12-31 10:38:02
11	com.facebook.auth.login	Facebook	action_account_add	2023-12-31 14:02:41
12	com.twitter.android.auth.login	SamsungAnd85032	action_account_add	2023-12-31 14:03:55
13	com.microsoft.skydrive	Smartphonedfir@outlook.com	action_account_add	2023-12-31 14:06:33
14	com.facebook.auth.login	61554997476190	action_account_add	2023-12-31 19:03:45

Wi-Fi networks

- **WiFiConfigStore.xml**
- Store Wi-Fi networks to which the phone was previously connected
- File is device-encrypted → **not protected with user passcode**
- XML format, **including password in clear text**

```
▼<Network>
  ▼<WifiConfiguration>
      <string name="ConfigKey">"Vodafone-C01670250"WPA_PSK</string>
      <string name="SSID">"Vodafone-C01670250"</string>
      <string name="PreSharedKey">"p3rZ6q4qT4nNAh4t"</string>
```

Bluetooth Devices

- **bt_config.conf**
- Paired Bluetooth devices
- File is Device Encrypted → **not protected with user passcode**

MAC Address	Name	Last Seen Date/Time
90:F1:57:F4:94:78	vívoactive 4	07/07/2024 14:26:58.000
D4:3A:2C:6E:0B:A9	Google Pixel Watch 045G	27/01/2024 02:07:12.000
94:45:60:1B:98:CC		
B4:EC:02:73:FF:93	Rouge	
14:22:3B:D1:E5:05	Pixel Buds A-Series	

Application usage

- **Usage Stats**
- App launch count and total time active in seconds
- Retention is up to **1 year**

Last Time Active	Usage Type	Time Active in Msecs	Time Active in Secs	Last Time Service Used	Last Time Visible	Total Time Visible	App Launch Count	Package	Types	Class	Source
2023-12-31 10:27:28	packages	65124	65				6	com.microsoft.teams			yearly
2023-12-31 12:59:24	packages	170278	170				4	com.microsoft.office.outlook			yearly
2023-12-31 15:33:36	packages	195687	195				8	com.facebook.orca			yearly
2023-12-31 15:34:00	packages	89	0				2	com.android.intentresolver			yearly
2023-12-31 15:34:27	packages	68737	68				7	com.dropbox.android			yearly

Application usage

- **Privacy Dashboard**
- Tracks the use of dangerous permissions (locations, camera, microphone)
- Retention is up to **1 week**

Timestamp	Bundle	Module	Operation	Usage in Seconds
2024-01-02 21:03:50	com.google.android.settings.intelligence		Location	
2023-12-29 15:12:31	com.whatsapp		Camera	
2023-12-30 10:00:05	com.android.chrome		Camera	186.8
2023-12-31 09:42:06	com.google.android.GoogleCamera		Camera	0.9
2023-12-31 13:14:26	vivino.web.app		Camera	522.8
2023-12-31 15:33:04	org.telegram.messenger		Camera	312.1
2023-12-31 16:28:36	org.thoughtcrime.securesms		Camera	182.1
2023-12-31 16:34:00	com.bereal.ft		Camera	122.4
2023-12-31 17:53:43	com.snapchat.android		Camera	220.7
2024-01-02 08:40:16	com.snapchat.android		Camera	23.3

Application usage

- **Digital Wellbeing**
- Various events (app in foreground, app in background, notification, device lock, device unlock, device startup, device shutdown)
- Retention is **7 to 30 days**, depending on the manufacturer

268574	28/07/2024 03:30:36.668	android	DEVICE_STARTUP	
268575	28/07/2024 03:30:36.744	com.android.settings	ACTIVITY_PAUSED	com.android.settings
268576	28/07/2024 03:30:36.871	com.google.android.apps.nexuslauncher	ACTIVITY_RESUMED	com.google.android.apps.nexuslauncher
268577	28/07/2024 03:30:37.292	android	KEYGUARD_HIDDEN	
268578	28/07/2024 03:30:37.797	com.android.settings	ACTIVITY_STOPPED	com.android.settings
268579	28/07/2024 03:30:41.172	com.google.android.apps.wear.companion	NOTIFICATION_INTERRUPTION	
268580	28/07/2024 03:30:41.185	com.google.android.apps.wear.companion	NOTIFICATION_INTERRUPTION	
268581	28/07/2024 03:30:46.623	com.silentcircle.silentphone	FOREGROUND_SERVICE_START	
268582	28/07/2024 03:30:46.813	com.silentcircle.silentphone	NOTIFICATION_INTERRUPTION	
268583	28/07/2024 03:30:47.541	com.google.android.apps.nexuslauncher	ACTIVITY_PAUSED	com.google.android.apps.nexuslauncher
268584	28/07/2024 03:30:47.545	com.garmin.android.apps.connectmobile	ACTIVITY_RESUMED	com.garmin.android.apps.connectmob...

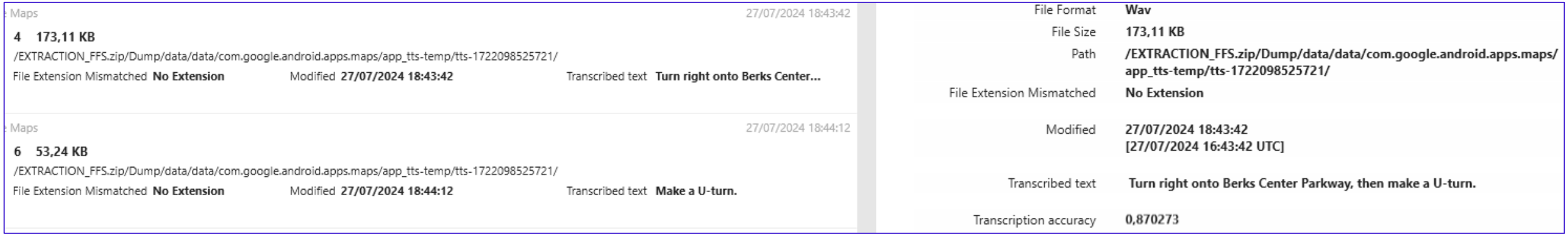
Geolocation

- **Google Timeline Events**
  - Latitude
  - Longitude
  - Accuracy (meters)
- Up to **30 days**

Latitude	Longitude	Accuracy (meters)	Visited Date/...
38.7811698	-77.2485147	100.0	28/07/2024 00:09:45.951
38.7811698	-77.2485147	24.699	27/07/2024 23:59:47.386
38.7811839	-77.2484873	100.0	27/07/2024 23:50:42.959
38.7811839	-77.2484873	17.556	27/07/2024 23:40:43.973
38.7811776	-77.2485023	100.0	27/07/2024 23:31:40.720
38.7811776	-77.2485023	21.149	27/07/2024 23:21:41.649
38.7811761	-77.2485101	20.0	27/07/2024 23:16:07.827
38.7811637	-77.2485062	26.101	27/07/2024 23:16:07.827
38.781176	-77.2485088	20.0	27/07/2024 23:16:07.827
38.7811766	-77.248494	20.0	27/07/2024 23:16:07.827
38.781219	-77.2484835	25.364	27/07/2024 23:16:07.827

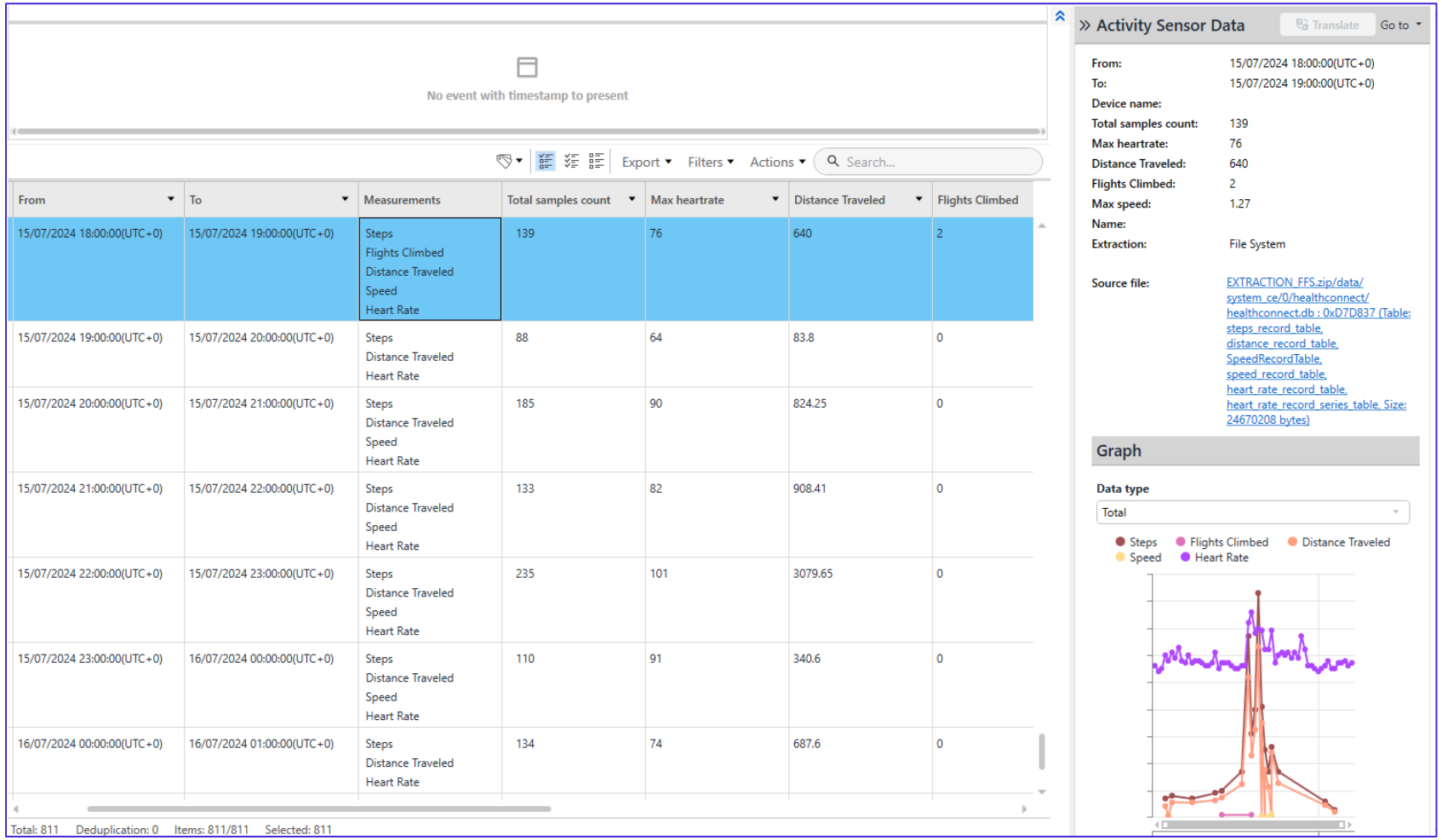
Geolocation

- **Google Maps turn-by-turn indication**
- The cache folder **stores data for months**
- Timestamps and audio file



Health

- **healthconnect.db**
- Unlimited retention
- Steps
- Distance
- Speed
- Hearth rate



Application data

- **Credential Encrypted →** You can decrypt if you know the passcode or you extract encryption keys (AFU)
- Contacts
- Call logs
- Messages
- Emails
- Notes
- Web activities
- Multimedia files

WhatsApp Accounts Information - Android	1
WhatsApp Calls	8
WhatsApp Chats - Android	12
WhatsApp Contacts - Android	92
WhatsApp Groups - Android	4
WhatsApp Messages - Android	577
WhatsApp Profile Pictures - Android	43
WhatsApp User Profiles - Android	1

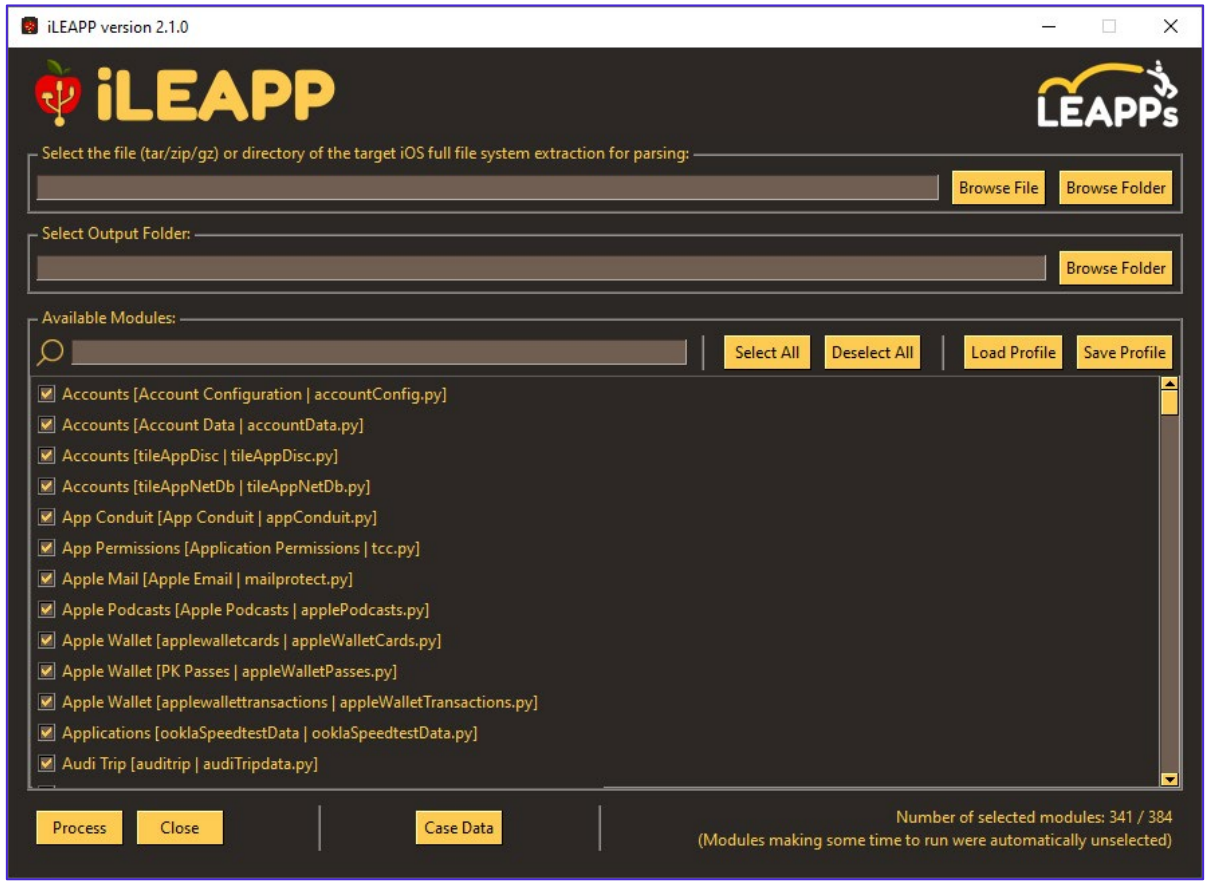
Pictures	83,071
Private Photo Vault Albums	2
Private Photo Vault Media	3
Private Photo Vault Thumbnails - Android	3
Videos	515

Chrome Affiliations	1
Chrome Autofill	4
Chrome Cache Records	3,034
Chrome Cookies	952
Chrome Current Tabs	7
Chrome Downloads	4
Chrome Favicons	76
Chrome Keyword Search Terms	7
Chrome Last Tabs	4
Chrome Logins	3
Chrome Saved Credit Cards	1
Chrome Tab History	24
Chrome Top Sites	2
Chrome Web History	51
Chrome Web Visits	57

RSAC™ 2025 Conference

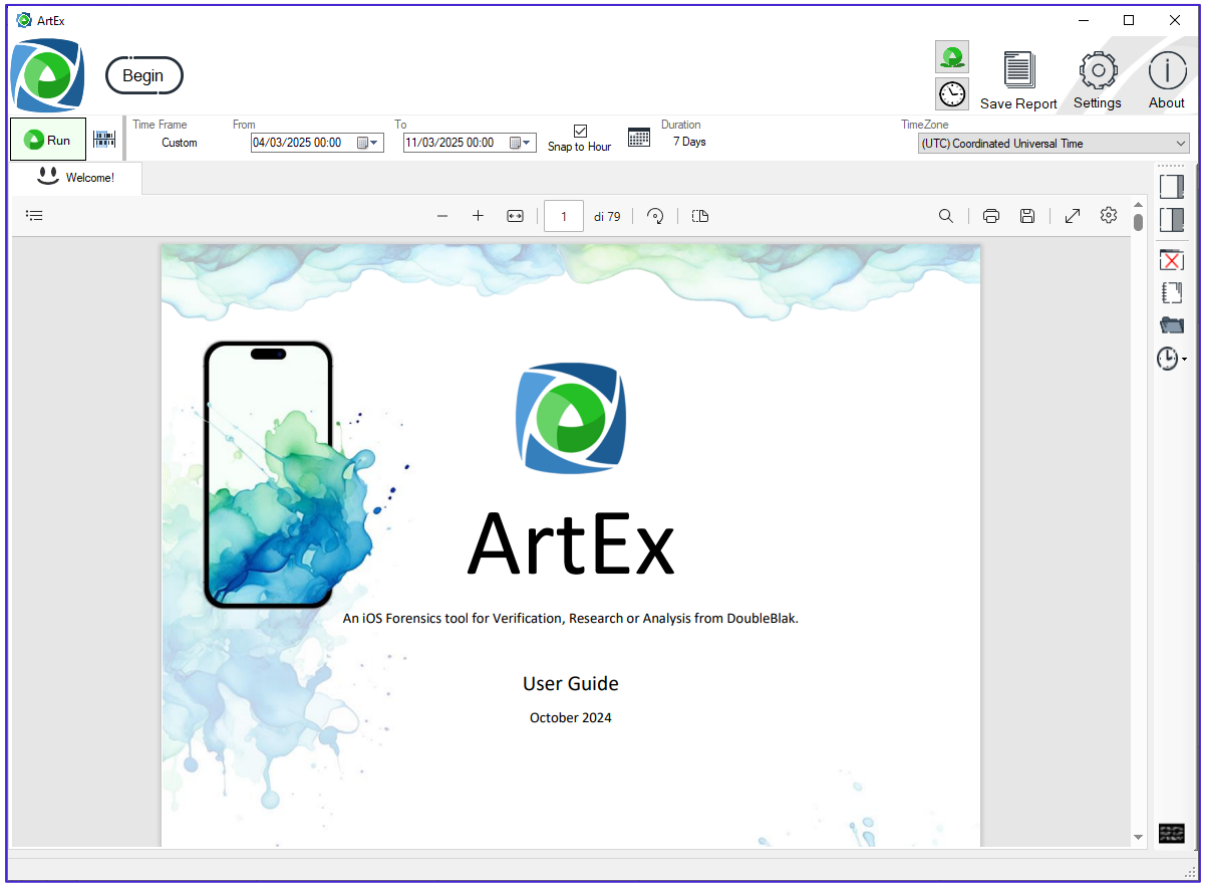
iOS

iLEAPP


iLEAPP version 2.1.0
iLEAPP
LEAPPs
Select the file (tar/zip/gz) or directory of the target iOS full file system extraction for parsing:
Browse File
Browse Folder
Select Output Folder:
Browse Folder
Available Modules:
Select All
Deselect All
Load Profile
Save Profile
Accounts [Account Configuration | accountConfig.py]
Accounts [Account Data | accountData.py]
Accounts [tileAppDisc | tileAppDisc.py]
Accounts [tileAppNetDb | tileAppNetDb.py]
App Conduit [App Conduit | appConduit.py]
App Permissions [Application Permissions | tcc.py]
Apple Mail [Apple Email | mailprotect.py]
Apple Podcasts [Apple Podcasts | applePodcasts.py]
Apple Wallet [applewalletcards | appleWalletCards.py]
Apple Wallet [PK Passes | appleWalletPasses.py]
Apple Wallet [applewallettransactions | appleWalletTransactions.py]
Applications [ooklaSpeedtestData | ooklaSpeedtestData.py]
Audi Trip [auditrip | audiTripdata.py]
Process
Close
Case Data
Number of selected modules: 341 / 384
(Modules making some time to run were automatically unselected)

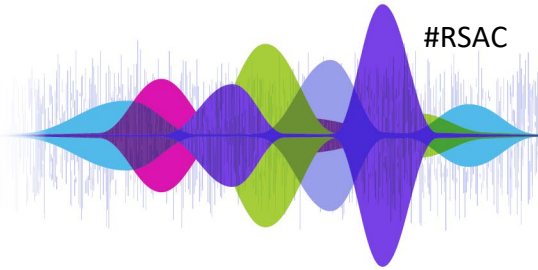
https://github.com/abrignoni/iLEAPP

ArtEx



https://doubleblak.com/

Installed and uninstalled applications



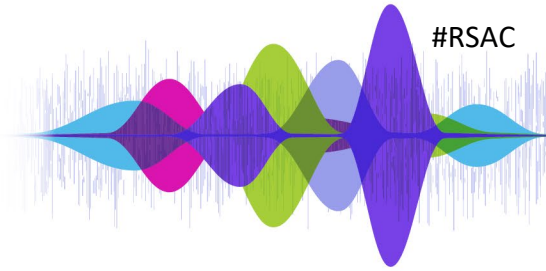
- **Mobile Installation Logs**
- Tracks application install and uninstall

Timestamp	Event	Bundle ID	Event Path
2023-12-08 21:57:21	Made container live	ph.telegra.Telegraph	/private/var/mobile/Containers/Data/Application/50D37839-46E5-4C29-81EE-C41123867FF9
2023-12-08 21:57:21	Made container live	ph.telegra.Telegraph	/private/var/containers/Bundle/Application/B489E9DD-062F-42A3-A79C-98B943BDD342
2023-12-08 21:57:21	Install successful	ph.telegra.Telegraph	
2023-12-08 21:58:21	Data container moved	ph.telegra.Telegraph	/private/var/mobile/Containers/Data/Application/818EF037-299B-4BFB-BE6C-BCB42E0C0BC4
2023-12-08 21:58:21	Made container live	ph.telegra.Telegraph.BroadcastUpload	/private/var/mobile/Containers/Data/PluginKitPlugin/7BFF0948-6B7B-40D9-982D-CAEB99BF750D
2023-12-08 21:58:21	Made container live	ph.telegra.Telegraph.NotificationContent	/private/var/mobile/Containers/Data/PluginKitPlugin/1EE61A47-CBE5-472C-8832-D7FFE499B0E4
2023-12-08 21:58:21	Made container live	ph.telegra.Telegraph.Widget	/private/var/mobile/Containers/Data/PluginKitPlugin/A2FC0CA8-0FD9-4D18-AB20-C1798652BE5B
2023-12-08 21:58:21	Made container live	ph.telegra.Telegraph.SiriIntents	/private/var/mobile/Containers/Data/PluginKitPlugin/22A84C89-6D54-415F-B5B2-45CA828D65B8
2023-12-08 21:58:21	Made container live	ph.telegra.Telegraph.NotificationService	/private/var/mobile/Containers/Data/PluginKitPlugin/AFE39B64-1204-4597-A4A5-47026A4BC78A
2023-12-08 21:58:21	Made container live	ph.telegra.Telegraph.Share	/private/var/mobile/Containers/Data/PluginKitPlugin/DD73681F-FCBB-4F08-AFFD-7D7422954719
2023-12-08 21:58:21	Made container live	ph.telegra.Telegraph	/private/var/containers/Bundle/Application/9E87D0C7-912F-4E28-A112-5F62818E8DDB
2023-12-08 21:58:21	Install successful	ph.telegra.Telegraph	
2023-12-13 22:41:55	Uninstalling identifier	ph.telegra.Telegraph	
2023-12-13 22:41:55	Destroying container	ph.telegra.Telegraph	/private/var/containers/Bundle/Application/9E87D0C7-912F-4E28-A112-5F62818E8DDB
2023-12-13 22:41:55	Destroying container	ph.telegra.Telegraph	/private/var/containers/Bundle/Application/9E87D0C7-912F-4E28-A112-5F62818E8DDB

Wi-Fi Networks

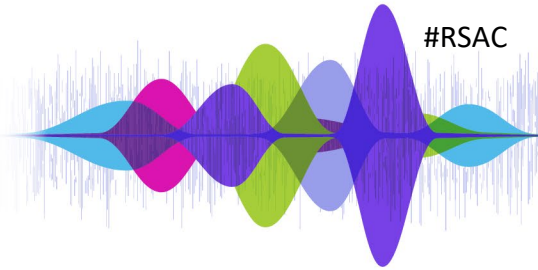
SSID	BSSID	Last Updated	Last Auto Joined	Last Joined	System Joined	User Joined	WiFi Network Password Modification Date	Last Discovered	Added At	Whitelisted Captive Network Probe Date	Captive Web Sheet Login Date	Previous Joined
#MSY-FI	74:88:bb:4c:12:af	2020-02-02 01:00:11+00:00	2020-02-09 15:23:54+00:00	2020-02-02 01:00:11+00:00								2020-02-09 15:08:10+00:00
#MSY-FI	74:88:bb:4c:12:af				2020-02-09 15:23:54+00:00	2020-02-02 01:00:11+00:00			2020-02-02 01:00:11+00:00			
#SFO FREE WIFI	0:4e:35:db:32:d1	2023-04-28 21:07:00+00:00			2023-04-28 21:02:52+00:00	2023-04-24 02:08:36+00:00		2023-04-28 17:56:15+00:00	2022-09-13 16:51:36+00:00	2023-04-28 20:22:42+00:00	2023-04-28 17:56:21+00:00	2023-04-28 20:38:52+00:00
.RSACONFERENCE	48:c0:93:6a:83:f0	2023-04-27 21:17:37+00:00			2023-04-27 20:34:55+00:00	2023-04-24 14:57:50+00:00		2023-04-27 18:50:48+00:00	2023-04-24 14:57:50+00:00	2023-04-27 15:46:25+00:00	2023-04-24 14:58:01+00:00	2023-04-27 20:33:02+00:00
@DatDog Free WiFi	ac:86:74:8b:d6:90	2020-02-07 02:14:51+00:00	2020-02-07 03:46:45+00:00	2020-02-07 02:14:51+00:00								2020-02-07 02:14:51+00:00
@DatDog Free WiFi	ac:86:74:8b:d6:90				2020-02-07 03:46:45+00:00	2020-02-07 02:14:51+00:00			2020-02-07 02:14:51+00:00			2020-02-07 02:14:51+00:00
@NOSHNola Guest	6:8d:db:17:54:ee	2020-02-06 02:07:08+00:00	2020-02-06 03:12:49+00:00	2020-02-06 02:07:08+00:00								
@NOSHNola Guest	6:8d:db:17:54:ee				2020-02-06 03:12:49+00:00	2020-02-06 02:07:08+00:00			2020-02-06 02:07:08+00:00			
@Sears Fine Guest WiFi	f0:b4:29:d1:d:ef	2023-04-26 14:23:35+00:00				2023-04-26 14:23:23+00:00			2023-04-26 14:23:23+00:00			
@SlushNola - Guest	e6:cb:ac:49:ec:67	2020-02-08 04:55:27+00:00	2020-02-09 04:48:10+00:00	2020-02-08 04:55:27+00:00								
@SlushNola - Guest	e6:cb:ac:49:ec:67				2020-02-09 04:48:10+00:00	2020-02-08 04:55:27+00:00			2020-02-08 04:55:27+00:00			
_Free JFK WiFi	70:b3:17:91:e0:2b	2020-02-01 19:01:32+00:00	2020-02-09 21:02:30+00:00	2020-02-01 19:24:05+00:00								2020-02-09 20:23:46+00:00

Bluetooth devices



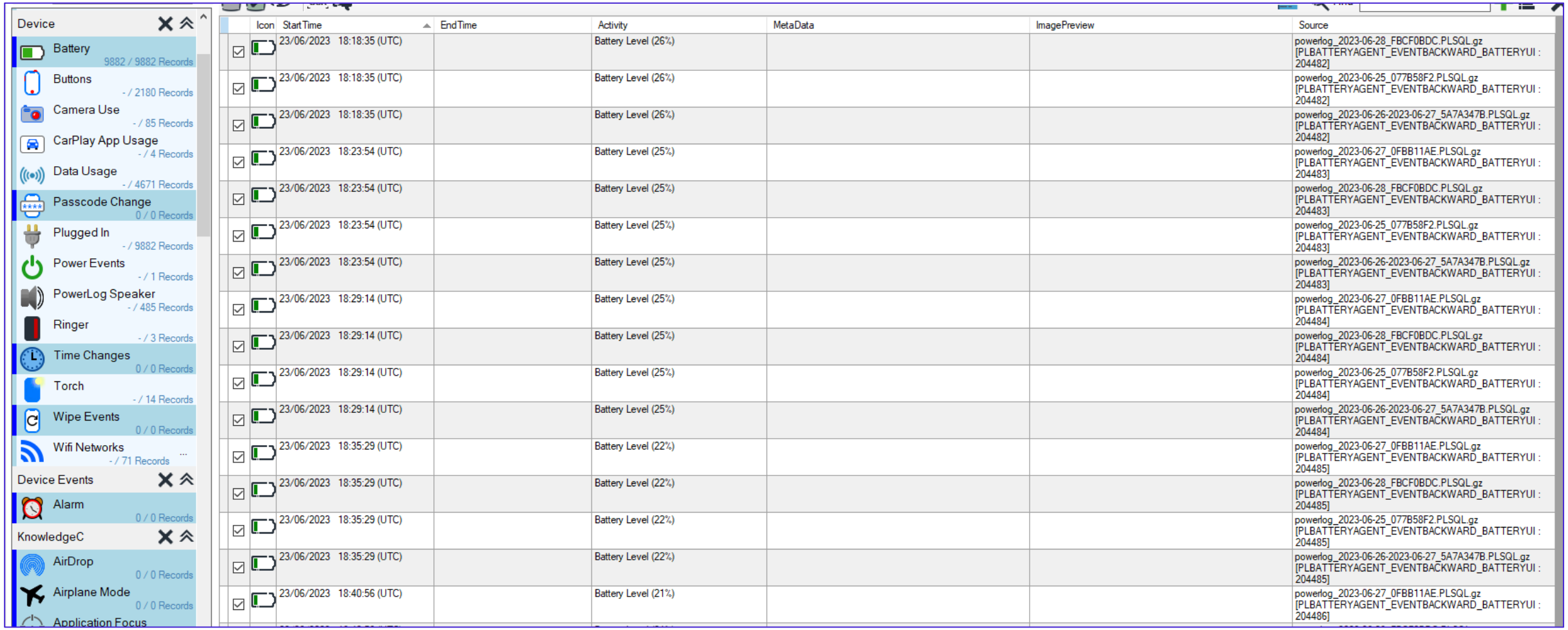
Last Seen Time	MAC Address	Name Key	Name	Device Product ID	Default Name
	9C:2E:A1:FA:E9:B0				
	B8:41:A4:12:E6:B7		Apple Watch		
	3C:39:C8:35:BB:F6		Apple Watch		
2020-11-01 22:50:36	4E:19:07:03:00:66		T8-R	291	Headset
2020-11-11 21:41:01	F0:13:C3:CA:F6:C4		HUAWEI AM08		Headset
2022-07-24 21:30:30	04:52:C7:A9:A5:19		Bose Mini II SoundLink	16393	Misc
2023-05-27 18:27:58	B4:EC:02:B3:00:8F		Toyota Touch		Handsfree
2023-06-21 09:56:42	00:1D:86:FC:23:81		KD-R7**BT	134	Headset
2023-06-30 18:30:41	3C:4D:BE:42:BF:99	Mattia's AirPods Pro	AirPods Pro	8206	Headphones

Device and application usage

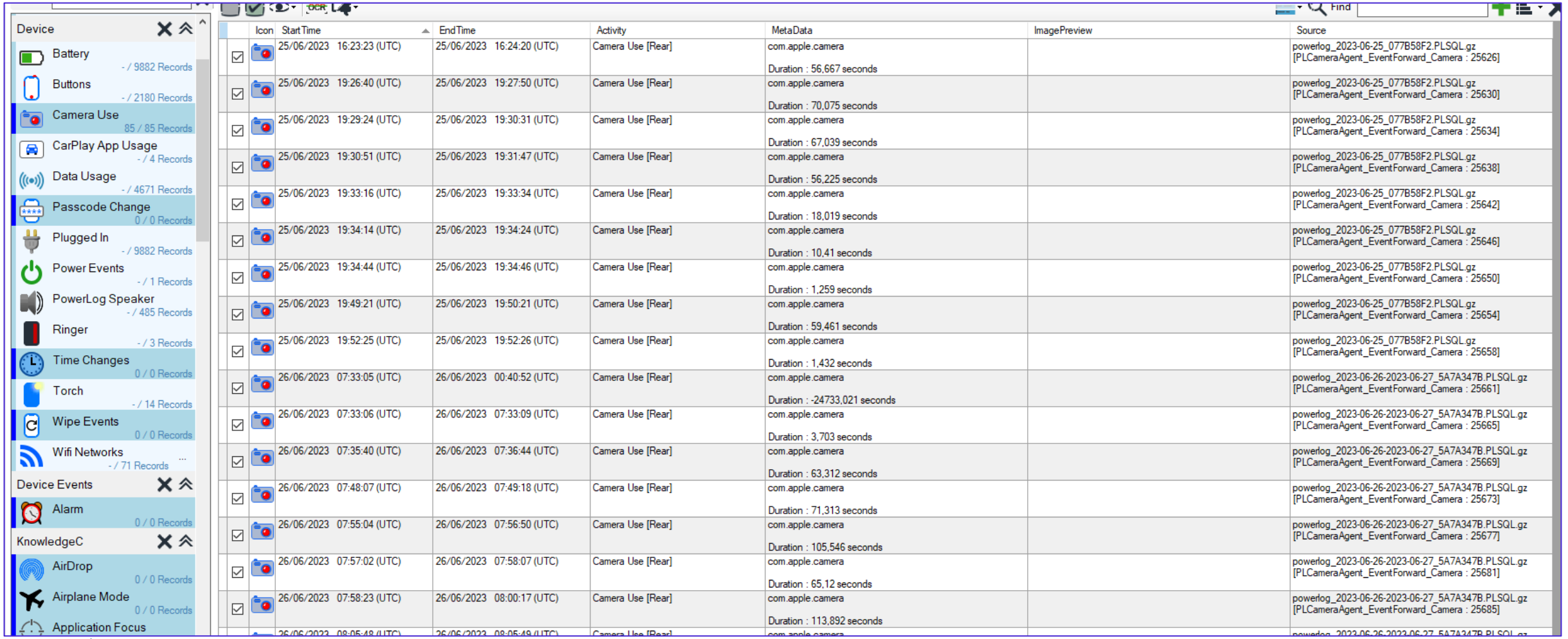


- **Power Log**
- Retention is **between 3 and 7 days** (depends upon usage)
  - Battery Level
  - Camera Use
  - Buttons (Pressed / Released)
  - Plugged / Unplugged
  - Torch On / Off
  - Lock State (Locked/Unlocked)

Battery Level

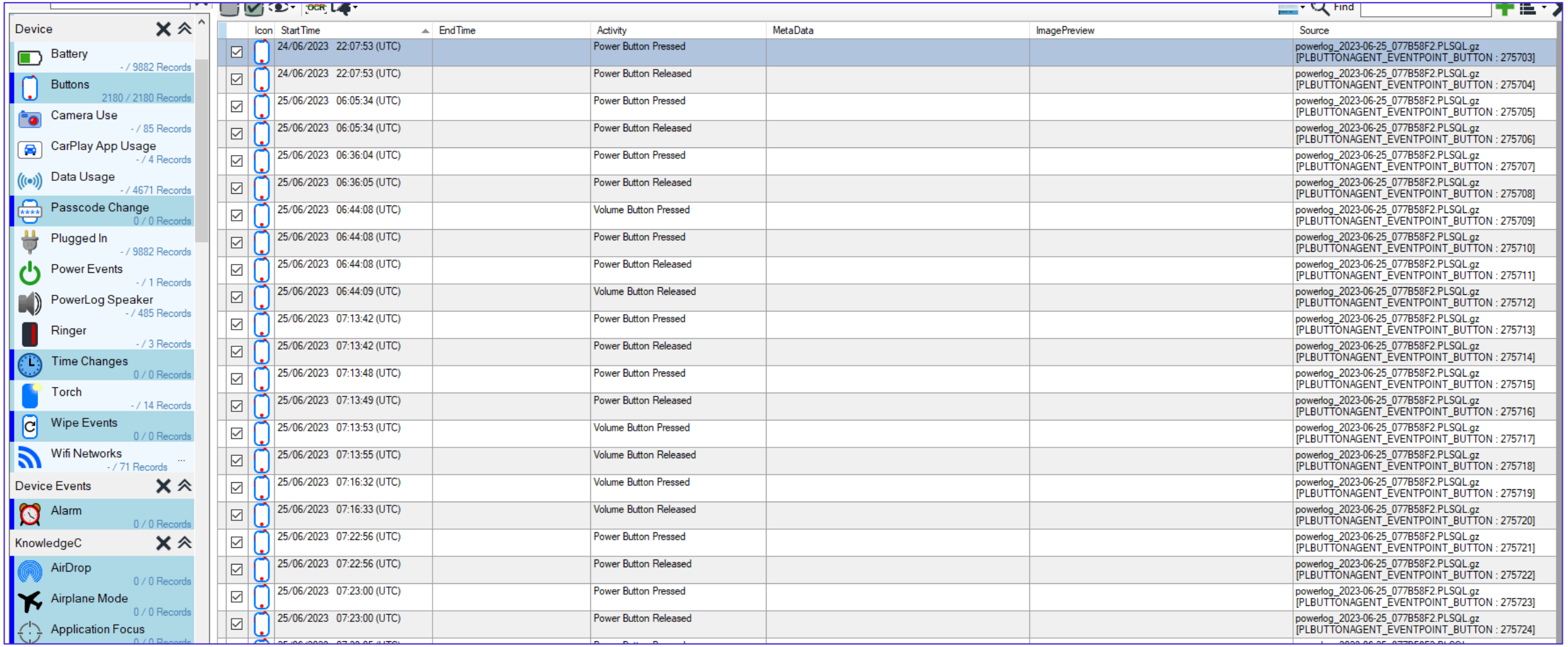


Camera Use

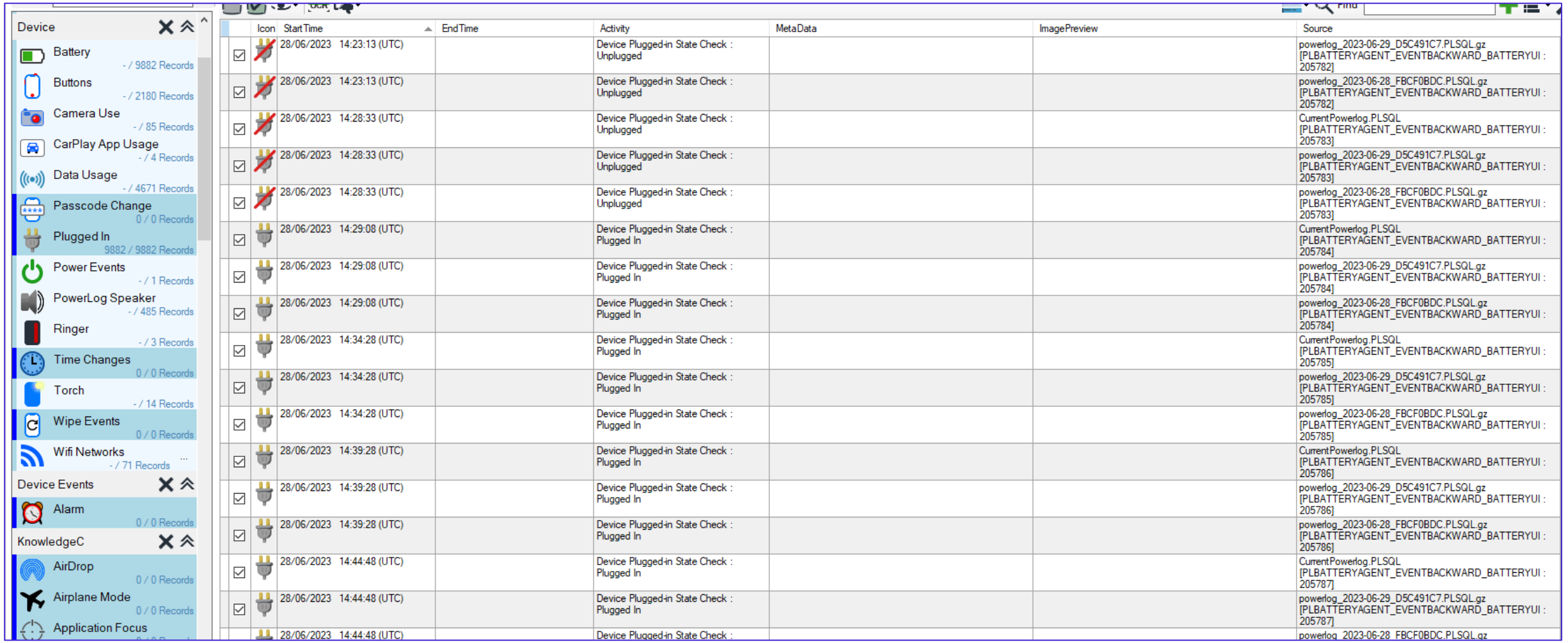

Device
Battery - / 9882 Records
Buttons - / 2180 Records
Camera Use 85 / 85 Records
CarPlay App Usage - / 4 Records
Data Usage - / 4671 Records
Passcode Change 0 / 0 Records
Plugged In - / 9882 Records
Power Events - / 1 Records
PowerLog Speaker - / 485 Records
Ringer - / 3 Records
Time Changes 0 / 0 Records
Torch - / 14 Records
Wipe Events 0 / 0 Records
Wifi Networks - / 71 Records
Device Events
Alarm 0 / 0 Records
KnowledgeC
AirDrop 0 / 0 Records
Airplane Mode 0 / 0 Records
Application Focus
Find

Icon	StartTime	EndTime	Activity	MetaData	ImagePreview	Source
☑	25/06/2023 16:23:23 (UTC)	25/06/2023 16:24:20 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 56,667 seconds		powerlog_2023-06-25_077B58F2.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25626]
☑	25/06/2023 19:26:40 (UTC)	25/06/2023 19:27:50 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 70,075 seconds		powerlog_2023-06-25_077B58F2.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25630]
☑	25/06/2023 19:29:24 (UTC)	25/06/2023 19:30:31 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 67,039 seconds		powerlog_2023-06-25_077B58F2.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25634]
☑	25/06/2023 19:30:51 (UTC)	25/06/2023 19:31:47 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 56,225 seconds		powerlog_2023-06-25_077B58F2.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25638]
☑	25/06/2023 19:33:16 (UTC)	25/06/2023 19:33:34 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 18,019 seconds		powerlog_2023-06-25_077B58F2.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25642]
☑	25/06/2023 19:34:14 (UTC)	25/06/2023 19:34:24 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 10,41 seconds		powerlog_2023-06-25_077B58F2.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25646]
☑	25/06/2023 19:34:44 (UTC)	25/06/2023 19:34:46 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 1,259 seconds		powerlog_2023-06-25_077B58F2.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25650]
☑	25/06/2023 19:49:21 (UTC)	25/06/2023 19:50:21 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 59,461 seconds		powerlog_2023-06-25_077B58F2.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25654]
☑	25/06/2023 19:52:25 (UTC)	25/06/2023 19:52:26 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 1,432 seconds		powerlog_2023-06-25_077B58F2.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25658]
☑	26/06/2023 07:33:05 (UTC)	26/06/2023 00:40:52 (UTC)	Camera Use [Rear]	com.apple.camera Duration : -24733,021 seconds		powerlog_2023-06-26-2023-06-27_5A7A347B.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25661]
☑	26/06/2023 07:33:06 (UTC)	26/06/2023 07:33:09 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 3,703 seconds		powerlog_2023-06-26-2023-06-27_5A7A347B.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25665]
☑	26/06/2023 07:35:40 (UTC)	26/06/2023 07:36:44 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 63,312 seconds		powerlog_2023-06-26-2023-06-27_5A7A347B.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25669]
☑	26/06/2023 07:48:07 (UTC)	26/06/2023 07:49:18 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 71,313 seconds		powerlog_2023-06-26-2023-06-27_5A7A347B.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25673]
☑	26/06/2023 07:55:04 (UTC)	26/06/2023 07:56:50 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 105,546 seconds		powerlog_2023-06-26-2023-06-27_5A7A347B.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25677]
☑	26/06/2023 07:57:02 (UTC)	26/06/2023 07:58:07 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 65,12 seconds		powerlog_2023-06-26-2023-06-27_5A7A347B.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25681]
☑	26/06/2023 07:58:23 (UTC)	26/06/2023 08:00:17 (UTC)	Camera Use [Rear]	com.apple.camera Duration : 113,892 seconds		powerlog_2023-06-26-2023-06-27_5A7A347B.PLSQL.gz [PLCameraAgent_EventForward_Camera : 25685]

Buttons (pressed/released)

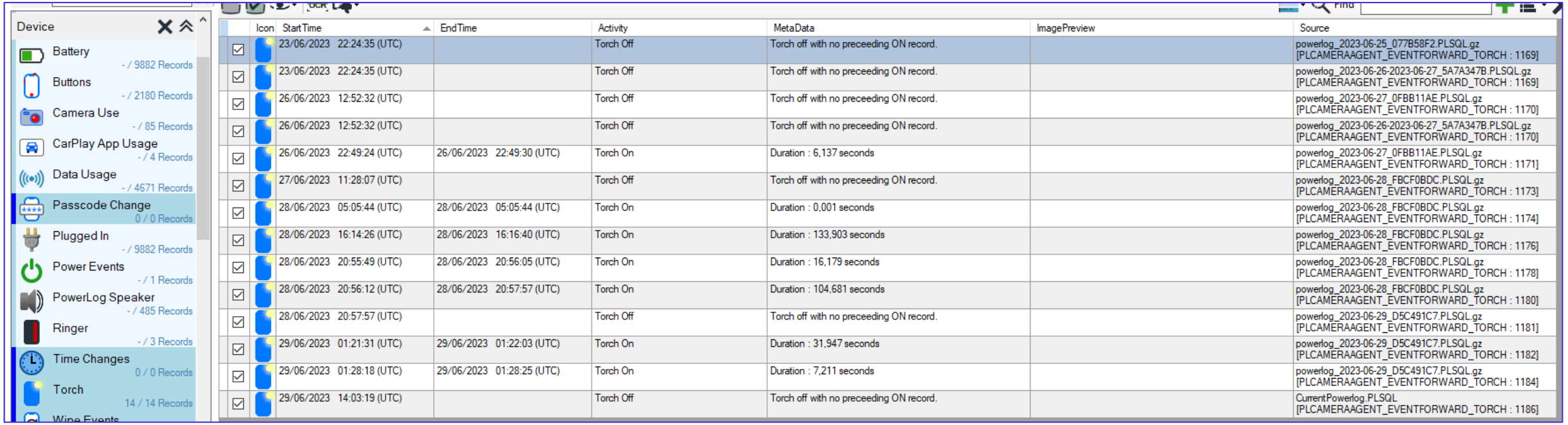

Device
Battery - / 9882 Records
Buttons 2180 / 2180 Records
Camera Use - / 85 Records
CarPlay App Usage - / 4 Records
Data Usage - / 4671 Records
Passcode Change 0 / 0 Records
Plugged In - / 9882 Records
Power Events - / 1 Records
PowerLog Speaker - / 485 Records
Ringer - / 3 Records
Time Changes 0 / 0 Records
Torch - / 14 Records
Wipe Events 0 / 0 Records
Wifi Networks - / 71 Records
Device Events
Alarm 0 / 0 Records
KnowledgeC
AirDrop 0 / 0 Records
Airplane Mode 0 / 0 Records
Application Focus
Find
Icon | StartTime | EndTime | Activity | MetaData | ImagePreview | Source
24/06/2023 22:07:53 (UTC) | Power Button Pressed | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275703]
24/06/2023 22:07:53 (UTC) | Power Button Released | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275704]
25/06/2023 06:05:34 (UTC) | Power Button Pressed | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275705]
25/06/2023 06:05:34 (UTC) | Power Button Released | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275706]
25/06/2023 06:36:04 (UTC) | Power Button Pressed | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275707]
25/06/2023 06:36:05 (UTC) | Power Button Released | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275708]
25/06/2023 06:44:08 (UTC) | Volume Button Pressed | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275709]
25/06/2023 06:44:08 (UTC) | Power Button Pressed | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275710]
25/06/2023 06:44:08 (UTC) | Power Button Released | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275711]
25/06/2023 06:44:09 (UTC) | Volume Button Released | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275712]
25/06/2023 07:13:42 (UTC) | Power Button Pressed | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275713]
25/06/2023 07:13:42 (UTC) | Power Button Released | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275714]
25/06/2023 07:13:48 (UTC) | Power Button Pressed | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275715]
25/06/2023 07:13:49 (UTC) | Power Button Released | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275716]
25/06/2023 07:13:53 (UTC) | Volume Button Pressed | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275717]
25/06/2023 07:13:55 (UTC) | Volume Button Released | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275718]
25/06/2023 07:16:32 (UTC) | Volume Button Pressed | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275719]
25/06/2023 07:16:33 (UTC) | Volume Button Released | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275720]
25/06/2023 07:22:56 (UTC) | Power Button Pressed | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275721]
25/06/2023 07:22:56 (UTC) | Power Button Released | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275722]
25/06/2023 07:23:00 (UTC) | Power Button Pressed | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275723]
25/06/2023 07:23:00 (UTC) | Power Button Released | powerlog_2023-06-25_077B58F2.PLSQL.gz [PLBUTTONAGENT_EVENTPOINT_BUTTON : 275724]

Plugged / Unplugged


Device
Battery - / 9882 Records
Buttons - / 2180 Records
Camera Use - / 85 Records
CarPlay App Usage - / 4 Records
Data Usage - / 4671 Records
Passcode Change 0 / 0 Records
Plugged In 9882 / 9882 Records
Power Events - / 1 Records
PowerLog Speaker - / 485 Records
Ringer - / 3 Records
Time Changes 0 / 0 Records
Torch - / 14 Records
Wipe Events 0 / 0 Records
Wifi Networks - / 71 Records
Device Events
Alarm 0 / 0 Records
KnowledgeC
AirDrop 0 / 0 Records
Airplane Mode 0 / 0 Records
Application Focus

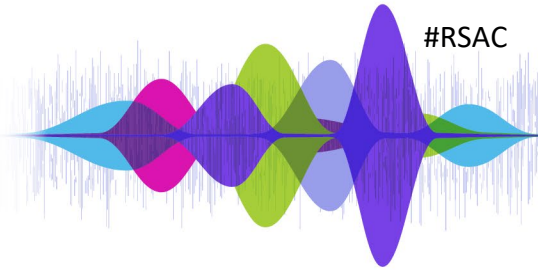
Icon	StartTime	EndTime	Activity	MetaData	ImagePreview	Source
	28/06/2023 14:23:13 (UTC)		Device Plugged-in State Check : Unplugged			powerlog_2023-06-29_D5C491C7.PLSQL.gz [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205782]
	28/06/2023 14:23:13 (UTC)		Device Plugged-in State Check : Unplugged			powerlog_2023-06-28_FBCF0BDC.PLSQL.gz [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205782]
	28/06/2023 14:28:33 (UTC)		Device Plugged-in State Check : Unplugged			CurrentPowerlog.PLSQL [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205783]
	28/06/2023 14:28:33 (UTC)		Device Plugged-in State Check : Unplugged			powerlog_2023-06-29_D5C491C7.PLSQL.gz [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205783]
	28/06/2023 14:28:33 (UTC)		Device Plugged-in State Check : Unplugged			powerlog_2023-06-28_FBCF0BDC.PLSQL.gz [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205783]
	28/06/2023 14:29:08 (UTC)		Device Plugged-in State Check : Plugged In			CurrentPowerlog.PLSQL [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205784]
	28/06/2023 14:29:08 (UTC)		Device Plugged-in State Check : Plugged In			powerlog_2023-06-29_D5C491C7.PLSQL.gz [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205784]
	28/06/2023 14:29:08 (UTC)		Device Plugged-in State Check : Plugged In			powerlog_2023-06-28_FBCF0BDC.PLSQL.gz [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205784]
	28/06/2023 14:34:28 (UTC)		Device Plugged-in State Check : Plugged In			CurrentPowerlog.PLSQL [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205785]
	28/06/2023 14:34:28 (UTC)		Device Plugged-in State Check : Plugged In			powerlog_2023-06-29_D5C491C7.PLSQL.gz [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205785]
	28/06/2023 14:34:28 (UTC)		Device Plugged-in State Check : Plugged In			powerlog_2023-06-28_FBCF0BDC.PLSQL.gz [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205785]
	28/06/2023 14:39:28 (UTC)		Device Plugged-in State Check : Plugged In			CurrentPowerlog.PLSQL [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205786]
	28/06/2023 14:39:28 (UTC)		Device Plugged-in State Check : Plugged In			powerlog_2023-06-29_D5C491C7.PLSQL.gz [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205786]
	28/06/2023 14:39:28 (UTC)		Device Plugged-in State Check : Plugged In			powerlog_2023-06-28_FBCF0BDC.PLSQL.gz [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205786]
	28/06/2023 14:44:48 (UTC)		Device Plugged-in State Check : Plugged In			CurrentPowerlog.PLSQL [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205787]
	28/06/2023 14:44:48 (UTC)		Device Plugged-in State Check : Plugged In			powerlog_2023-06-29_D5C491C7.PLSQL.gz [PLBATTERYAGENT_EVENTBACKWARD_BATTERYUI : 205787]
	28/06/2023 14:44:48 (UTC)		Device Plugged-in State Check :			powerlog_2023-06-28_FBCF0BDC.PLSQL.gz

Torch On/Off



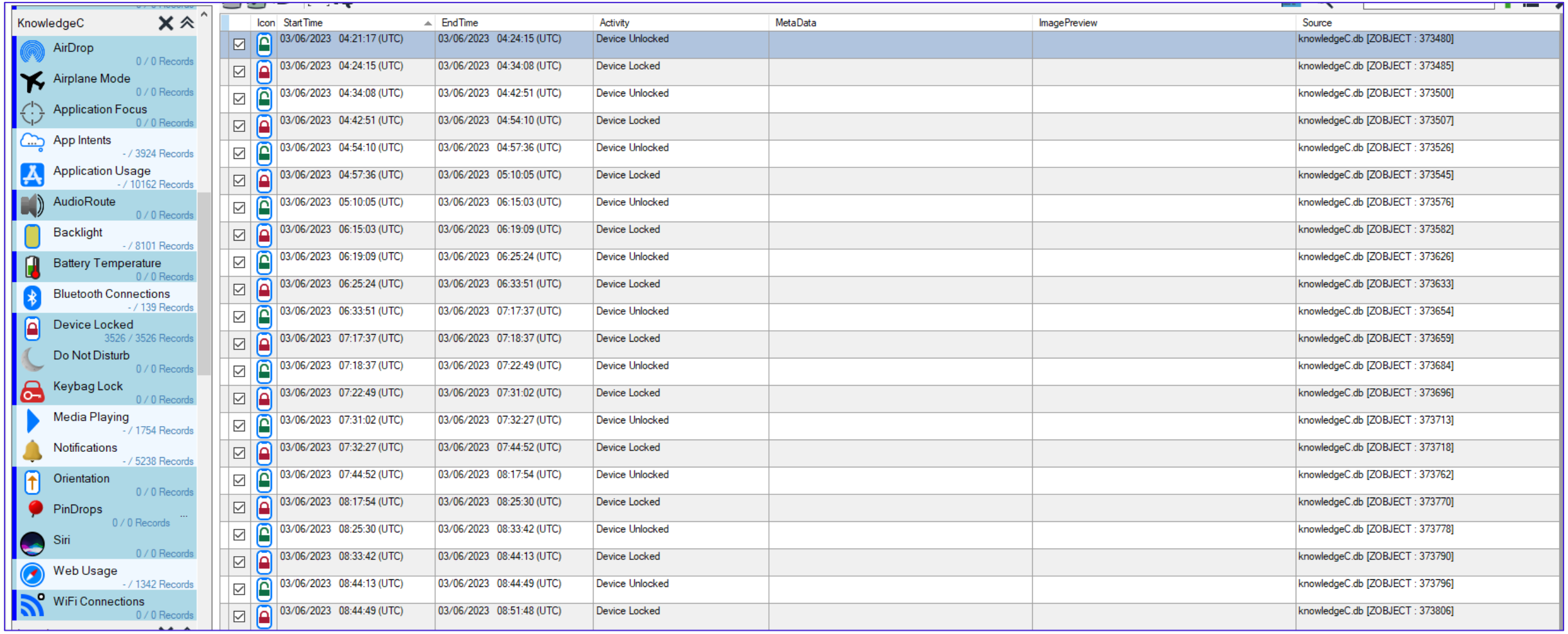
Icon	StartTime	EndTime	Activity	MetaData	ImagePreview	Source
	23/06/2023 22:24:35 (UTC)		Torch Off	Torch off with no preceeding ON record.		powerlog_2023-06-25_077B58F2.PLSQL.gz [PLCAMERAAGENT_EVENTFORWARD_TORCH : 1169]
	23/06/2023 22:24:35 (UTC)		Torch Off	Torch off with no preceeding ON record.		powerlog_2023-06-26-2023-06-27_5A7A347B.PLSQL.gz [PLCAMERAAGENT_EVENTFORWARD_TORCH : 1169]
	26/06/2023 12:52:32 (UTC)		Torch Off	Torch off with no preceeding ON record.		powerlog_2023-06-27_0FBB11AE.PLSQL.gz [PLCAMERAAGENT_EVENTFORWARD_TORCH : 1170]
	26/06/2023 12:52:32 (UTC)		Torch Off	Torch off with no preceeding ON record.		powerlog_2023-06-26-2023-06-27_5A7A347B.PLSQL.gz [PLCAMERAAGENT_EVENTFORWARD_TORCH : 1170]
	26/06/2023 22:49:24 (UTC)	26/06/2023 22:49:30 (UTC)	Torch On	Duration : 6,137 seconds		powerlog_2023-06-27_0FBB11AE.PLSQL.gz [PLCAMERAAGENT_EVENTFORWARD_TORCH : 1171]
	27/06/2023 11:28:07 (UTC)		Torch Off	Torch off with no preceeding ON record.		powerlog_2023-06-28_FBCF0BDC.PLSQL.gz [PLCAMERAAGENT_EVENTFORWARD_TORCH : 1173]
	28/06/2023 05:05:44 (UTC)	28/06/2023 05:05:44 (UTC)	Torch On	Duration : 0,001 seconds		powerlog_2023-06-28_FBCF0BDC.PLSQL.gz [PLCAMERAAGENT_EVENTFORWARD_TORCH : 1174]
	28/06/2023 16:14:26 (UTC)	28/06/2023 16:16:40 (UTC)	Torch On	Duration : 133,903 seconds		powerlog_2023-06-28_FBCF0BDC.PLSQL.gz [PLCAMERAAGENT_EVENTFORWARD_TORCH : 1176]
	28/06/2023 20:55:49 (UTC)	28/06/2023 20:56:05 (UTC)	Torch On	Duration : 16,179 seconds		powerlog_2023-06-28_FBCF0BDC.PLSQL.gz [PLCAMERAAGENT_EVENTFORWARD_TORCH : 1178]
	28/06/2023 20:56:12 (UTC)	28/06/2023 20:57:57 (UTC)	Torch On	Duration : 104,681 seconds		powerlog_2023-06-28_FBCF0BDC.PLSQL.gz [PLCAMERAAGENT_EVENTFORWARD_TORCH : 1180]
	28/06/2023 20:57:57 (UTC)		Torch Off	Torch off with no preceeding ON record.		powerlog_2023-06-29_D5C491C7.PLSQL.gz [PLCAMERAAGENT_EVENTFORWARD_TORCH : 1181]
	29/06/2023 01:21:31 (UTC)	29/06/2023 01:22:03 (UTC)	Torch On	Duration : 31,947 seconds		powerlog_2023-06-29_D5C491C7.PLSQL.gz [PLCAMERAAGENT_EVENTFORWARD_TORCH : 1182]
	29/06/2023 01:28:18 (UTC)	29/06/2023 01:28:25 (UTC)	Torch On	Duration : 7,211 seconds		powerlog_2023-06-29_D5C491C7.PLSQL.gz [PLCAMERAAGENT_EVENTFORWARD_TORCH : 1184]
	29/06/2023 14:03:19 (UTC)		Torch Off	Torch off with no preceeding ON record.		CurrentPowerlog.PLSQL [PLCAMERAAGENT_EVENTFORWARD_TORCH : 1186]

Device and application usage



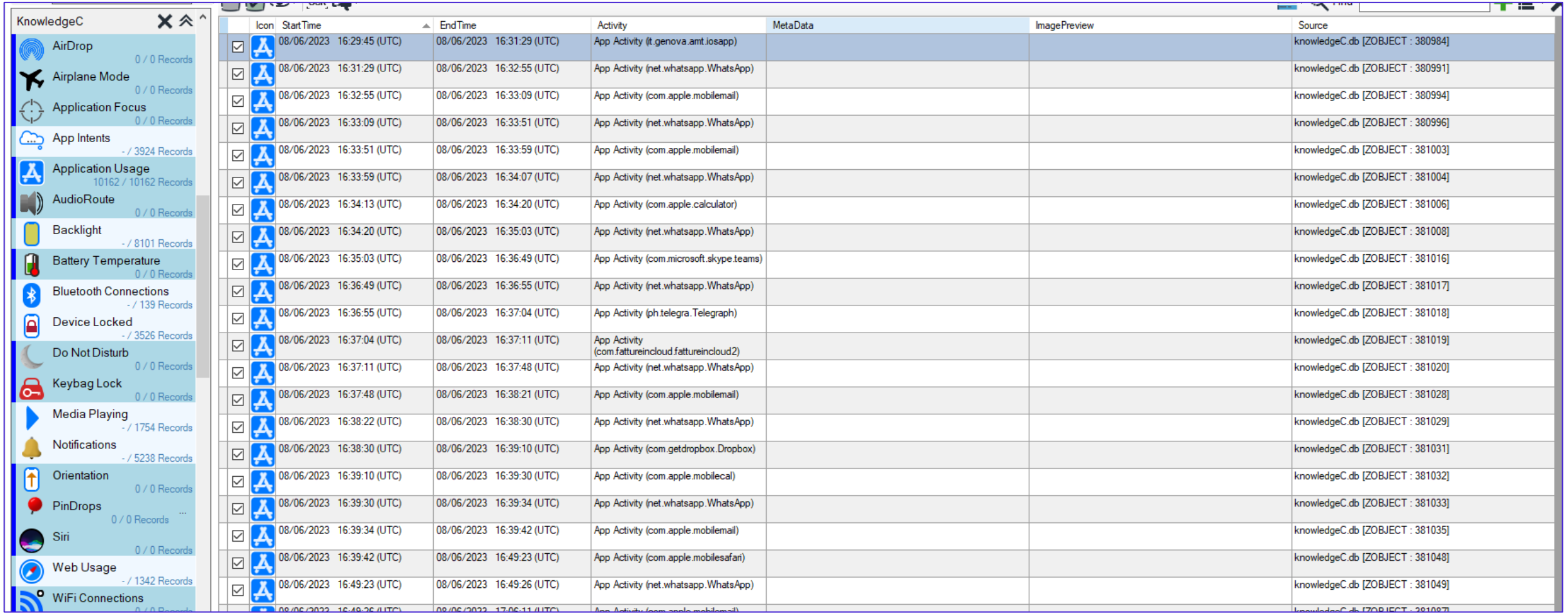
- **knowledgeC.db** (up to iOS 16)
- Retention is **28 days**
  - Device locked/unlocked
  - App “in focus”
  - Screen backlight (on/off)
  - Plugged in
  - Screen orientation
  - Bluetooth connections
  - Media playing
  - Notifications

Device locked/unlocked


KnowledgeC
AirDrop 0 / 0 Records
Airplane Mode 0 / 0 Records
Application Focus 0 / 0 Records
App Intents - / 3924 Records
Application Usage - / 10162 Records
AudioRoute 0 / 0 Records
Backlight - / 8101 Records
Battery Temperature 0 / 0 Records
Bluetooth Connections - / 139 Records
Device Locked 3526 / 3526 Records
Do Not Disturb 0 / 0 Records
Keybag Lock 0 / 0 Records
Media Playing - / 1754 Records
Notifications - / 5238 Records
Orientation 0 / 0 Records
PinDrops 0 / 0 Records
Siri 0 / 0 Records
Web Usage - / 1342 Records
WiFi Connections 0 / 0 Records

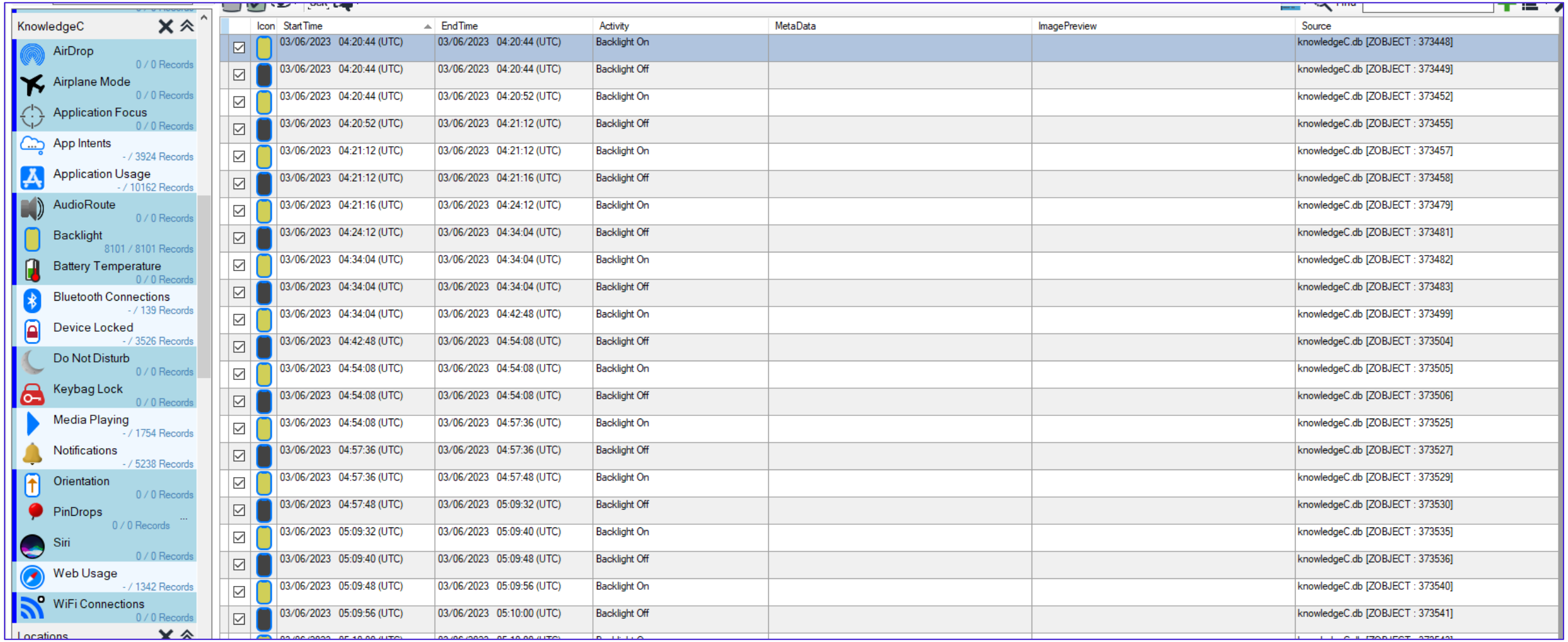
Icon	StartTime	EndTime	Activity	MetaData	ImagePreview	Source
	03/06/2023 04:21:17 (UTC)	03/06/2023 04:24:15 (UTC)	Device Unlocked			knowledgeC.db [ZOBJECT : 373480]
	03/06/2023 04:24:15 (UTC)	03/06/2023 04:34:08 (UTC)	Device Locked			knowledgeC.db [ZOBJECT : 373485]
	03/06/2023 04:34:08 (UTC)	03/06/2023 04:42:51 (UTC)	Device Unlocked			knowledgeC.db [ZOBJECT : 373500]
	03/06/2023 04:42:51 (UTC)	03/06/2023 04:54:10 (UTC)	Device Locked			knowledgeC.db [ZOBJECT : 373507]
	03/06/2023 04:54:10 (UTC)	03/06/2023 04:57:36 (UTC)	Device Unlocked			knowledgeC.db [ZOBJECT : 373526]
	03/06/2023 04:57:36 (UTC)	03/06/2023 05:10:05 (UTC)	Device Locked			knowledgeC.db [ZOBJECT : 373545]
	03/06/2023 05:10:05 (UTC)	03/06/2023 06:15:03 (UTC)	Device Unlocked			knowledgeC.db [ZOBJECT : 373576]
	03/06/2023 06:15:03 (UTC)	03/06/2023 06:19:09 (UTC)	Device Locked			knowledgeC.db [ZOBJECT : 373582]
	03/06/2023 06:19:09 (UTC)	03/06/2023 06:25:24 (UTC)	Device Unlocked			knowledgeC.db [ZOBJECT : 373626]
	03/06/2023 06:25:24 (UTC)	03/06/2023 06:33:51 (UTC)	Device Locked			knowledgeC.db [ZOBJECT : 373633]
	03/06/2023 06:33:51 (UTC)	03/06/2023 07:17:37 (UTC)	Device Unlocked			knowledgeC.db [ZOBJECT : 373654]
	03/06/2023 07:17:37 (UTC)	03/06/2023 07:18:37 (UTC)	Device Locked			knowledgeC.db [ZOBJECT : 373659]
	03/06/2023 07:18:37 (UTC)	03/06/2023 07:22:49 (UTC)	Device Unlocked			knowledgeC.db [ZOBJECT : 373684]
	03/06/2023 07:22:49 (UTC)	03/06/2023 07:31:02 (UTC)	Device Locked			knowledgeC.db [ZOBJECT : 373696]
	03/06/2023 07:31:02 (UTC)	03/06/2023 07:32:27 (UTC)	Device Unlocked			knowledgeC.db [ZOBJECT : 373713]
	03/06/2023 07:32:27 (UTC)	03/06/2023 07:44:52 (UTC)	Device Locked			knowledgeC.db [ZOBJECT : 373718]
	03/06/2023 07:44:52 (UTC)	03/06/2023 08:17:54 (UTC)	Device Unlocked			knowledgeC.db [ZOBJECT : 373762]
	03/06/2023 08:17:54 (UTC)	03/06/2023 08:25:30 (UTC)	Device Locked			knowledgeC.db [ZOBJECT : 373770]
	03/06/2023 08:25:30 (UTC)	03/06/2023 08:33:42 (UTC)	Device Unlocked			knowledgeC.db [ZOBJECT : 373778]
	03/06/2023 08:33:42 (UTC)	03/06/2023 08:44:13 (UTC)	Device Locked			knowledgeC.db [ZOBJECT : 373790]
	03/06/2023 08:44:13 (UTC)	03/06/2023 08:44:49 (UTC)	Device Unlocked			knowledgeC.db [ZOBJECT : 373796]
	03/06/2023 08:44:49 (UTC)	03/06/2023 08:51:48 (UTC)	Device Locked			knowledgeC.db [ZOBJECT : 373806]

App In Focus



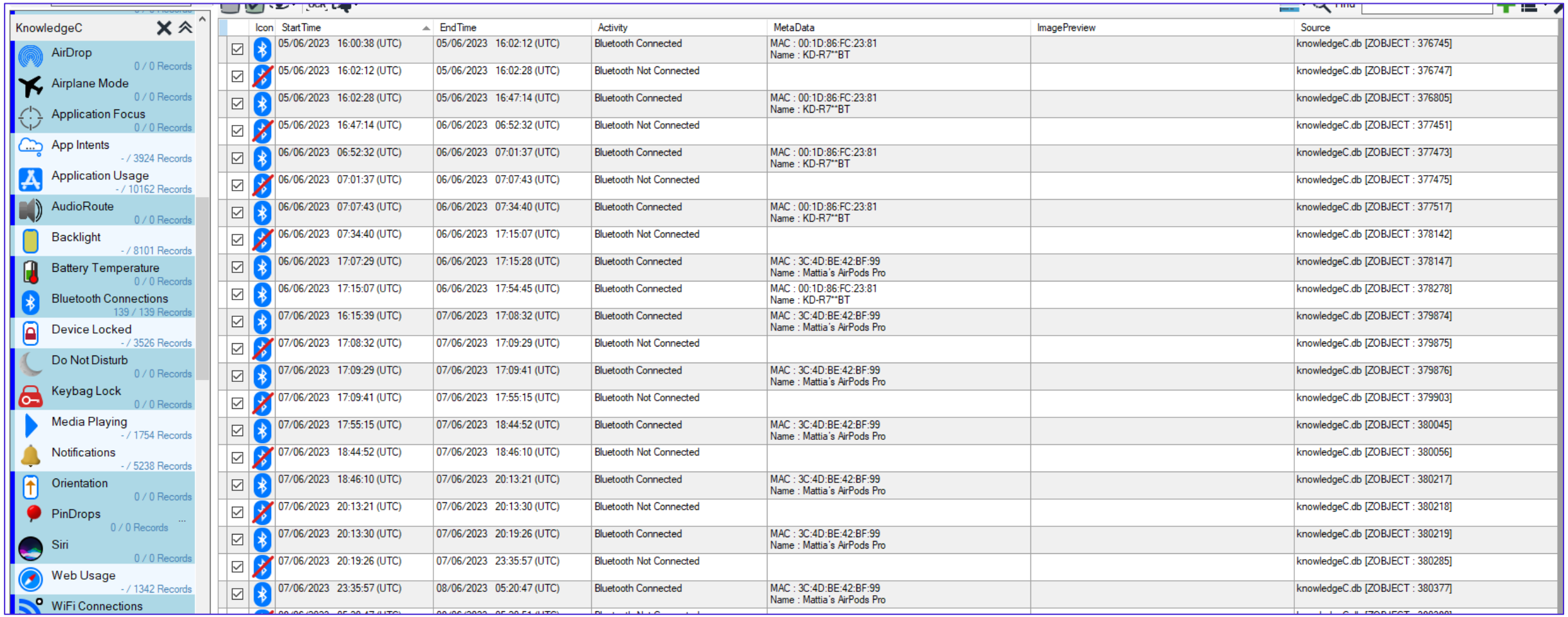
Icon	StartTime	EndTime	Activity	MetaData	ImagePreview	Source
	08/06/2023 16:29:45 (UTC)	08/06/2023 16:31:29 (UTC)	App Activity (it.genova.amt.iosapp)			knowledgeC.db [ZOBJECT : 380984]
	08/06/2023 16:31:29 (UTC)	08/06/2023 16:32:55 (UTC)	App Activity (net.whatsapp.WhatsApp)			knowledgeC.db [ZOBJECT : 380991]
	08/06/2023 16:32:55 (UTC)	08/06/2023 16:33:09 (UTC)	App Activity (com.apple.mobilemail)			knowledgeC.db [ZOBJECT : 380994]
	08/06/2023 16:33:09 (UTC)	08/06/2023 16:33:51 (UTC)	App Activity (net.whatsapp.WhatsApp)			knowledgeC.db [ZOBJECT : 380996]
	08/06/2023 16:33:51 (UTC)	08/06/2023 16:33:59 (UTC)	App Activity (com.apple.mobilemail)			knowledgeC.db [ZOBJECT : 381003]
	08/06/2023 16:33:59 (UTC)	08/06/2023 16:34:07 (UTC)	App Activity (net.whatsapp.WhatsApp)			knowledgeC.db [ZOBJECT : 381004]
	08/06/2023 16:34:13 (UTC)	08/06/2023 16:34:20 (UTC)	App Activity (com.apple.calculator)			knowledgeC.db [ZOBJECT : 381006]
	08/06/2023 16:34:20 (UTC)	08/06/2023 16:35:03 (UTC)	App Activity (net.whatsapp.WhatsApp)			knowledgeC.db [ZOBJECT : 381008]
	08/06/2023 16:35:03 (UTC)	08/06/2023 16:36:49 (UTC)	App Activity (com.microsoft.skype.teams)			knowledgeC.db [ZOBJECT : 381016]
	08/06/2023 16:36:49 (UTC)	08/06/2023 16:36:55 (UTC)	App Activity (net.whatsapp.WhatsApp)			knowledgeC.db [ZOBJECT : 381017]
	08/06/2023 16:36:55 (UTC)	08/06/2023 16:37:04 (UTC)	App Activity (ph.telegra.Telegraph)			knowledgeC.db [ZOBJECT : 381018]
	08/06/2023 16:37:04 (UTC)	08/06/2023 16:37:11 (UTC)	App Activity (com.fattureincloud.fattureincloud2)			knowledgeC.db [ZOBJECT : 381019]
	08/06/2023 16:37:11 (UTC)	08/06/2023 16:37:48 (UTC)	App Activity (net.whatsapp.WhatsApp)			knowledgeC.db [ZOBJECT : 381020]
	08/06/2023 16:37:48 (UTC)	08/06/2023 16:38:21 (UTC)	App Activity (com.apple.mobilemail)			knowledgeC.db [ZOBJECT : 381028]
	08/06/2023 16:38:22 (UTC)	08/06/2023 16:38:30 (UTC)	App Activity (net.whatsapp.WhatsApp)			knowledgeC.db [ZOBJECT : 381029]
	08/06/2023 16:38:30 (UTC)	08/06/2023 16:39:10 (UTC)	App Activity (com.getdropbox.Dropbox)			knowledgeC.db [ZOBJECT : 381031]
	08/06/2023 16:39:10 (UTC)	08/06/2023 16:39:30 (UTC)	App Activity (com.apple.mobilecal)			knowledgeC.db [ZOBJECT : 381032]
	08/06/2023 16:39:30 (UTC)	08/06/2023 16:39:34 (UTC)	App Activity (net.whatsapp.WhatsApp)			knowledgeC.db [ZOBJECT : 381033]
	08/06/2023 16:39:34 (UTC)	08/06/2023 16:39:42 (UTC)	App Activity (com.apple.mobilemail)			knowledgeC.db [ZOBJECT : 381035]
	08/06/2023 16:39:42 (UTC)	08/06/2023 16:49:23 (UTC)	App Activity (com.apple.mobilesafari)			knowledgeC.db [ZOBJECT : 381048]
	08/06/2023 16:49:23 (UTC)	08/06/2023 16:49:26 (UTC)	App Activity (net.whatsapp.WhatsApp)			knowledgeC.db [ZOBJECT : 381049]

Screen backlight (On/Off)



Icon	StartTime	EndTime	Activity	MetaData	ImagePreview	Source
	03/06/2023 04:20:44 (UTC)	03/06/2023 04:20:44 (UTC)	Backlight On			knowledgeC.db [ZOBJECT : 373448]
	03/06/2023 04:20:44 (UTC)	03/06/2023 04:20:44 (UTC)	Backlight Off			knowledgeC.db [ZOBJECT : 373449]
	03/06/2023 04:20:44 (UTC)	03/06/2023 04:20:52 (UTC)	Backlight On			knowledgeC.db [ZOBJECT : 373452]
	03/06/2023 04:20:52 (UTC)	03/06/2023 04:21:12 (UTC)	Backlight Off			knowledgeC.db [ZOBJECT : 373455]
	03/06/2023 04:21:12 (UTC)	03/06/2023 04:21:12 (UTC)	Backlight On			knowledgeC.db [ZOBJECT : 373457]
	03/06/2023 04:21:12 (UTC)	03/06/2023 04:21:16 (UTC)	Backlight Off			knowledgeC.db [ZOBJECT : 373458]
	03/06/2023 04:21:16 (UTC)	03/06/2023 04:24:12 (UTC)	Backlight On			knowledgeC.db [ZOBJECT : 373479]
	03/06/2023 04:24:12 (UTC)	03/06/2023 04:34:04 (UTC)	Backlight Off			knowledgeC.db [ZOBJECT : 373481]
	03/06/2023 04:34:04 (UTC)	03/06/2023 04:34:04 (UTC)	Backlight On			knowledgeC.db [ZOBJECT : 373482]
	03/06/2023 04:34:04 (UTC)	03/06/2023 04:34:04 (UTC)	Backlight Off			knowledgeC.db [ZOBJECT : 373483]
	03/06/2023 04:34:04 (UTC)	03/06/2023 04:42:48 (UTC)	Backlight On			knowledgeC.db [ZOBJECT : 373499]
	03/06/2023 04:42:48 (UTC)	03/06/2023 04:54:08 (UTC)	Backlight Off			knowledgeC.db [ZOBJECT : 373504]
	03/06/2023 04:54:08 (UTC)	03/06/2023 04:54:08 (UTC)	Backlight On			knowledgeC.db [ZOBJECT : 373505]
	03/06/2023 04:54:08 (UTC)	03/06/2023 04:54:08 (UTC)	Backlight Off			knowledgeC.db [ZOBJECT : 373506]
	03/06/2023 04:54:08 (UTC)	03/06/2023 04:57:36 (UTC)	Backlight On			knowledgeC.db [ZOBJECT : 373525]
	03/06/2023 04:57:36 (UTC)	03/06/2023 04:57:36 (UTC)	Backlight Off			knowledgeC.db [ZOBJECT : 373527]
	03/06/2023 04:57:36 (UTC)	03/06/2023 04:57:48 (UTC)	Backlight On			knowledgeC.db [ZOBJECT : 373529]
	03/06/2023 04:57:48 (UTC)	03/06/2023 05:09:32 (UTC)	Backlight Off			knowledgeC.db [ZOBJECT : 373530]
	03/06/2023 05:09:32 (UTC)	03/06/2023 05:09:40 (UTC)	Backlight On			knowledgeC.db [ZOBJECT : 373535]
	03/06/2023 05:09:40 (UTC)	03/06/2023 05:09:48 (UTC)	Backlight Off			knowledgeC.db [ZOBJECT : 373536]
	03/06/2023 05:09:48 (UTC)	03/06/2023 05:09:56 (UTC)	Backlight On			knowledgeC.db [ZOBJECT : 373540]
	03/06/2023 05:09:56 (UTC)	03/06/2023 05:10:00 (UTC)	Backlight Off			knowledgeC.db [ZOBJECT : 373541]

Bluetooth Connections



Icon	StartTime	EndTime	Activity	MetaData	ImagePreview	Source
	05/06/2023 16:00:38 (UTC)	05/06/2023 16:02:12 (UTC)	Bluetooth Connected	MAC : 00:1D:86:FC:23:81 Name : KD-R7**BT		knowledgeC.db [ZOBJECT : 376745]
	05/06/2023 16:02:12 (UTC)	05/06/2023 16:02:28 (UTC)	Bluetooth Not Connected			knowledgeC.db [ZOBJECT : 376747]
	05/06/2023 16:02:28 (UTC)	05/06/2023 16:47:14 (UTC)	Bluetooth Connected	MAC : 00:1D:86:FC:23:81 Name : KD-R7**BT		knowledgeC.db [ZOBJECT : 376805]
	05/06/2023 16:47:14 (UTC)	06/06/2023 06:52:32 (UTC)	Bluetooth Not Connected			knowledgeC.db [ZOBJECT : 377451]
	06/06/2023 06:52:32 (UTC)	06/06/2023 07:01:37 (UTC)	Bluetooth Connected	MAC : 00:1D:86:FC:23:81 Name : KD-R7**BT		knowledgeC.db [ZOBJECT : 377473]
	06/06/2023 07:01:37 (UTC)	06/06/2023 07:07:43 (UTC)	Bluetooth Not Connected			knowledgeC.db [ZOBJECT : 377475]
	06/06/2023 07:07:43 (UTC)	06/06/2023 07:34:40 (UTC)	Bluetooth Connected	MAC : 00:1D:86:FC:23:81 Name : KD-R7**BT		knowledgeC.db [ZOBJECT : 377517]
	06/06/2023 07:34:40 (UTC)	06/06/2023 17:15:07 (UTC)	Bluetooth Not Connected			knowledgeC.db [ZOBJECT : 378142]
	06/06/2023 17:07:29 (UTC)	06/06/2023 17:15:28 (UTC)	Bluetooth Connected	MAC : 3C:4D:BE:42:BF:99 Name : Mattia's AirPods Pro		knowledgeC.db [ZOBJECT : 378147]
	06/06/2023 17:15:07 (UTC)	06/06/2023 17:54:45 (UTC)	Bluetooth Connected	MAC : 00:1D:86:FC:23:81 Name : KD-R7**BT		knowledgeC.db [ZOBJECT : 378278]
	07/06/2023 16:15:39 (UTC)	07/06/2023 17:08:32 (UTC)	Bluetooth Connected	MAC : 3C:4D:BE:42:BF:99 Name : Mattia's AirPods Pro		knowledgeC.db [ZOBJECT : 379874]
	07/06/2023 17:08:32 (UTC)	07/06/2023 17:09:29 (UTC)	Bluetooth Not Connected			knowledgeC.db [ZOBJECT : 379875]
	07/06/2023 17:09:29 (UTC)	07/06/2023 17:09:41 (UTC)	Bluetooth Connected	MAC : 3C:4D:BE:42:BF:99 Name : Mattia's AirPods Pro		knowledgeC.db [ZOBJECT : 379876]
	07/06/2023 17:09:41 (UTC)	07/06/2023 17:55:15 (UTC)	Bluetooth Not Connected			knowledgeC.db [ZOBJECT : 379903]
	07/06/2023 17:55:15 (UTC)	07/06/2023 18:44:52 (UTC)	Bluetooth Connected	MAC : 3C:4D:BE:42:BF:99 Name : Mattia's AirPods Pro		knowledgeC.db [ZOBJECT : 380045]
	07/06/2023 18:44:52 (UTC)	07/06/2023 18:46:10 (UTC)	Bluetooth Not Connected			knowledgeC.db [ZOBJECT : 380056]
	07/06/2023 18:46:10 (UTC)	07/06/2023 20:13:21 (UTC)	Bluetooth Connected	MAC : 3C:4D:BE:42:BF:99 Name : Mattia's AirPods Pro		knowledgeC.db [ZOBJECT : 380217]
	07/06/2023 20:13:21 (UTC)	07/06/2023 20:13:30 (UTC)	Bluetooth Not Connected			knowledgeC.db [ZOBJECT : 380218]
	07/06/2023 20:13:30 (UTC)	07/06/2023 20:19:26 (UTC)	Bluetooth Connected	MAC : 3C:4D:BE:42:BF:99 Name : Mattia's AirPods Pro		knowledgeC.db [ZOBJECT : 380219]
	07/06/2023 20:19:26 (UTC)	07/06/2023 23:35:57 (UTC)	Bluetooth Not Connected			knowledgeC.db [ZOBJECT : 380285]
	07/06/2023 23:35:57 (UTC)	08/06/2023 05:20:47 (UTC)	Bluetooth Connected	MAC : 3C:4D:BE:42:BF:99 Name : Mattia's AirPods Pro		knowledgeC.db [ZOBJECT : 380377]

Media Playing (1)

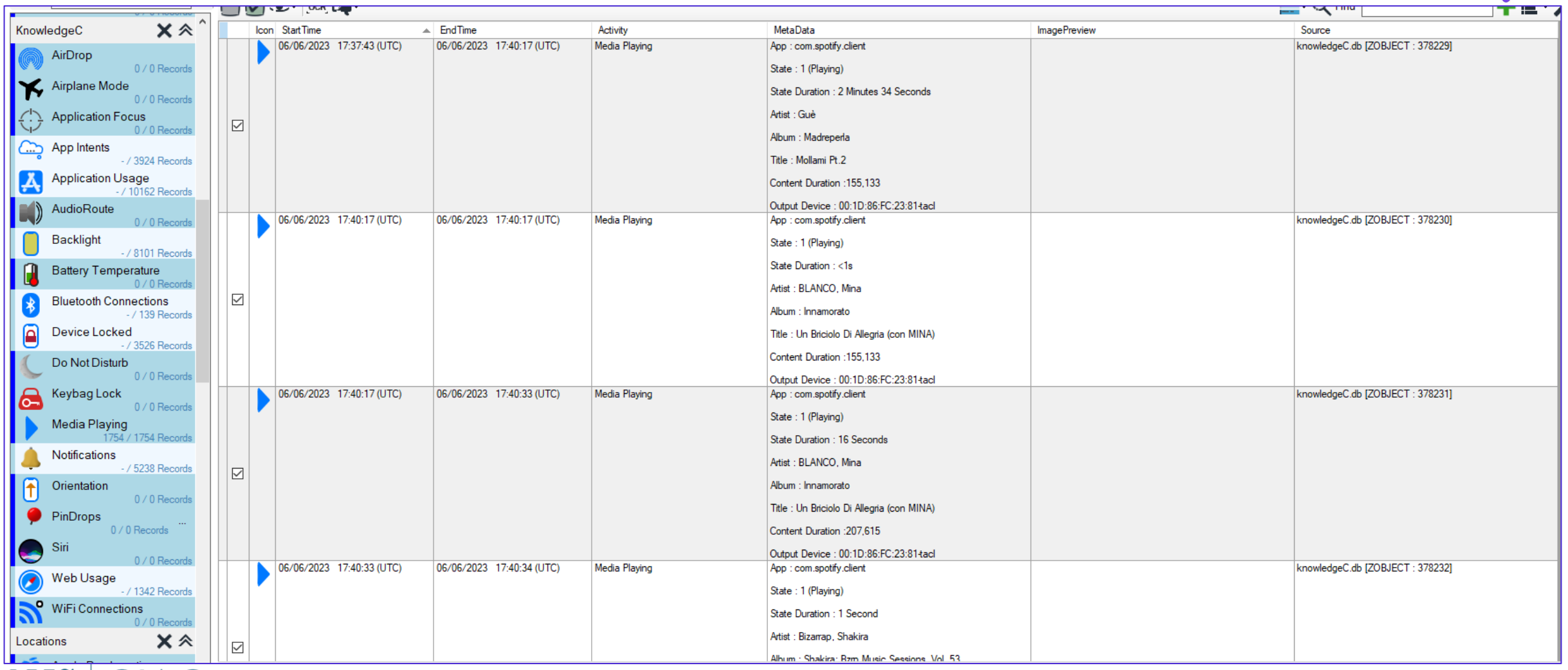
KnowledgeC

- AirDrop — 0 / 0 Records
- Airplane Mode — 0 / 0 Records
- Application Focus — 0 / 0 Records
- App Intents — - / 3924 Records
- Application Usage — - / 10162 Records
- AudioRoute — 0 / 0 Records
- Backlight — - / 8101 Records
- Battery Temperature — 0 / 0 Records
- Bluetooth Connections — - / 139 Records
- Device Locked — - / 3526 Records
- Do Not Disturb — 0 / 0 Records
- Keybag Lock — 0 / 0 Records
- Media Playing — 1754 / 1754 Records
- Notifications — - / 5238 Records
- Orientation — 0 / 0 Records
- PinDrops — 0 / 0 Records
- Siri — 0 / 0 Records
- Web Usage — - / 1342 Records
- WiFi Connections — 0 / 0 Records

Locations

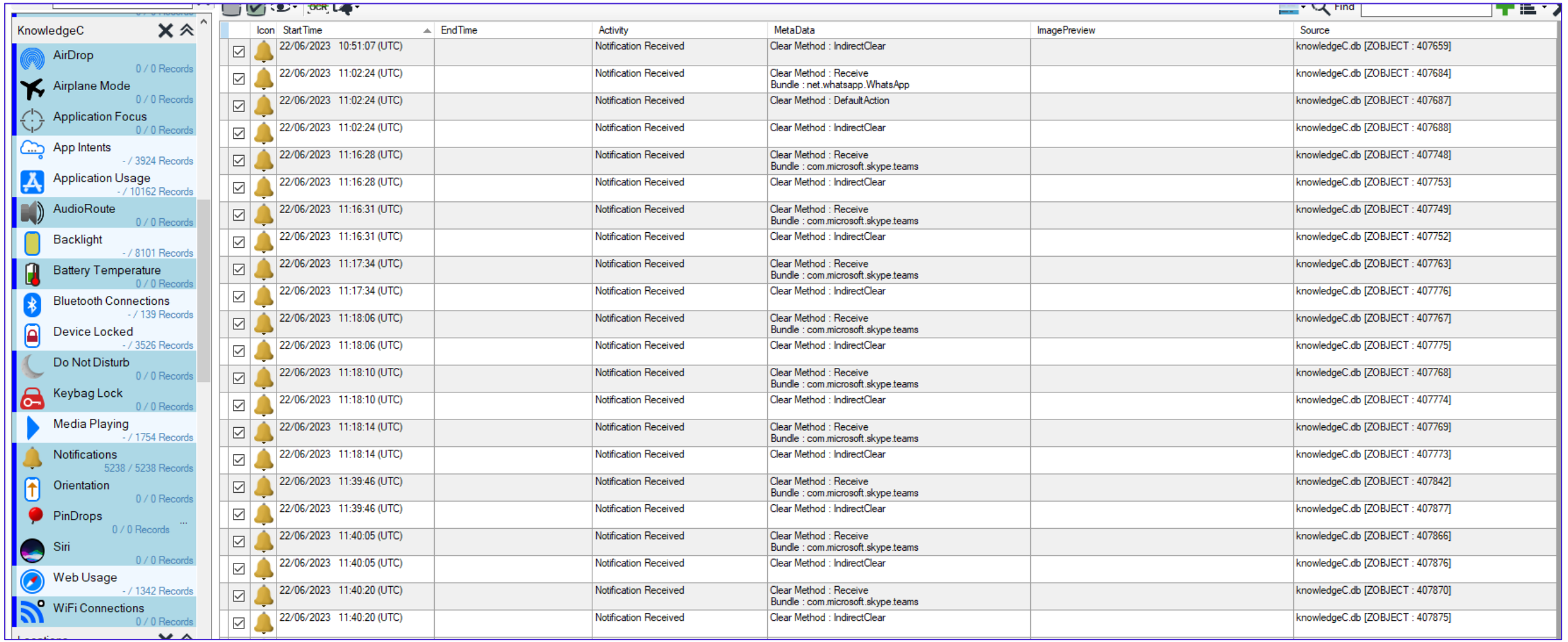
Icon	StartTime	EndTime	Activity	MetaData	ImagePreview	Source
▶	06/06/2023 17:15:21 (UTC)	06/06/2023 17:15:25 (UTC)	Media Playing	App : com.spotify.client State : 1 (Playing) State Duration : 4 Seconds Artist : Annalisa Album : Bellissima Title : Bellissima Content Duration :201,334 Output Device : 3C:4D:BE:42:BF:99-tacl		knowledgeC.db [ZOBJECT : 378145]
▶	06/06/2023 17:15:25 (UTC)	06/06/2023 17:15:26 (UTC)	Media Playing	App : com.spotify.client State : 1 (Playing) State Duration : 1 Second Artist : Annalisa Album : Bellissima Title : Bellissima Content Duration :201,334 Output Device : 00:1D:86:FC:23:81-tacl		knowledgeC.db [ZOBJECT : 378146]
▮▮	06/06/2023 17:15:26 (UTC)	06/06/2023 17:15:36 (UTC)	Media Playing	App : com.spotify.client State : 2 (Paused) State Duration : 10 Seconds Artist : Annalisa Album : Bellissima Title : Bellissima Content Duration :201,334 Output Device : 00:1D:86:FC:23:81-tacl		knowledgeC.db [ZOBJECT : 378149]
▶	06/06/2023 17:15:36 (UTC)	06/06/2023 17:16:20 (UTC)	Media Playing	App : com.spotify.client State : 1 (Playing) State Duration : 44 Seconds Artist : Annalisa Album : Bellissima		knowledgeC.db [ZOBJECT : 378152]

Media Playing (2)



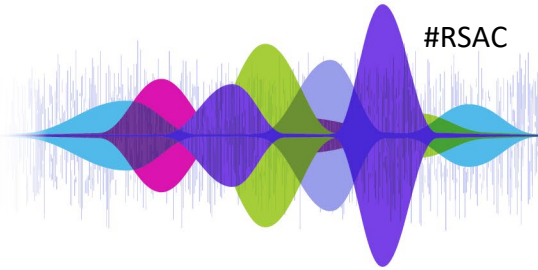
Icon	StartTime	EndTime	Activity	MetaData	ImagePreview	Source
	06/06/2023 17:37:43 (UTC)	06/06/2023 17:40:17 (UTC)	Media Playing	App : com.spotify.client State : 1 (Playing) State Duration : 2 Minutes 34 Seconds Artist : Guè Album : Madreperla Title : Mollami Pt.2 Content Duration :155,133 Output Device : 00:1D:86:FC:23:81-tacl		knowledgeC.db [ZOBJECT : 378229]
	06/06/2023 17:40:17 (UTC)	06/06/2023 17:40:17 (UTC)	Media Playing	App : com.spotify.client State : 1 (Playing) State Duration : <1s Artist : BLANCO, Mina Album : Innamorato Title : Un Briciolo Di Allegria (con MINA) Content Duration :155,133 Output Device : 00:1D:86:FC:23:81-tacl		knowledgeC.db [ZOBJECT : 378230]
	06/06/2023 17:40:17 (UTC)	06/06/2023 17:40:33 (UTC)	Media Playing	App : com.spotify.client State : 1 (Playing) State Duration : 16 Seconds Artist : BLANCO, Mina Album : Innamorato Title : Un Briciolo Di Allegria (con MINA) Content Duration :207,615 Output Device : 00:1D:86:FC:23:81-tacl		knowledgeC.db [ZOBJECT : 378231]
	06/06/2023 17:40:33 (UTC)	06/06/2023 17:40:34 (UTC)	Media Playing	App : com.spotify.client State : 1 (Playing) State Duration : 1 Second Artist : Bizarrap, Shakira Album : Shakira: Bzrp Music Sessions, Vol. 53		knowledgeC.db [ZOBJECT : 378232]

Notifications

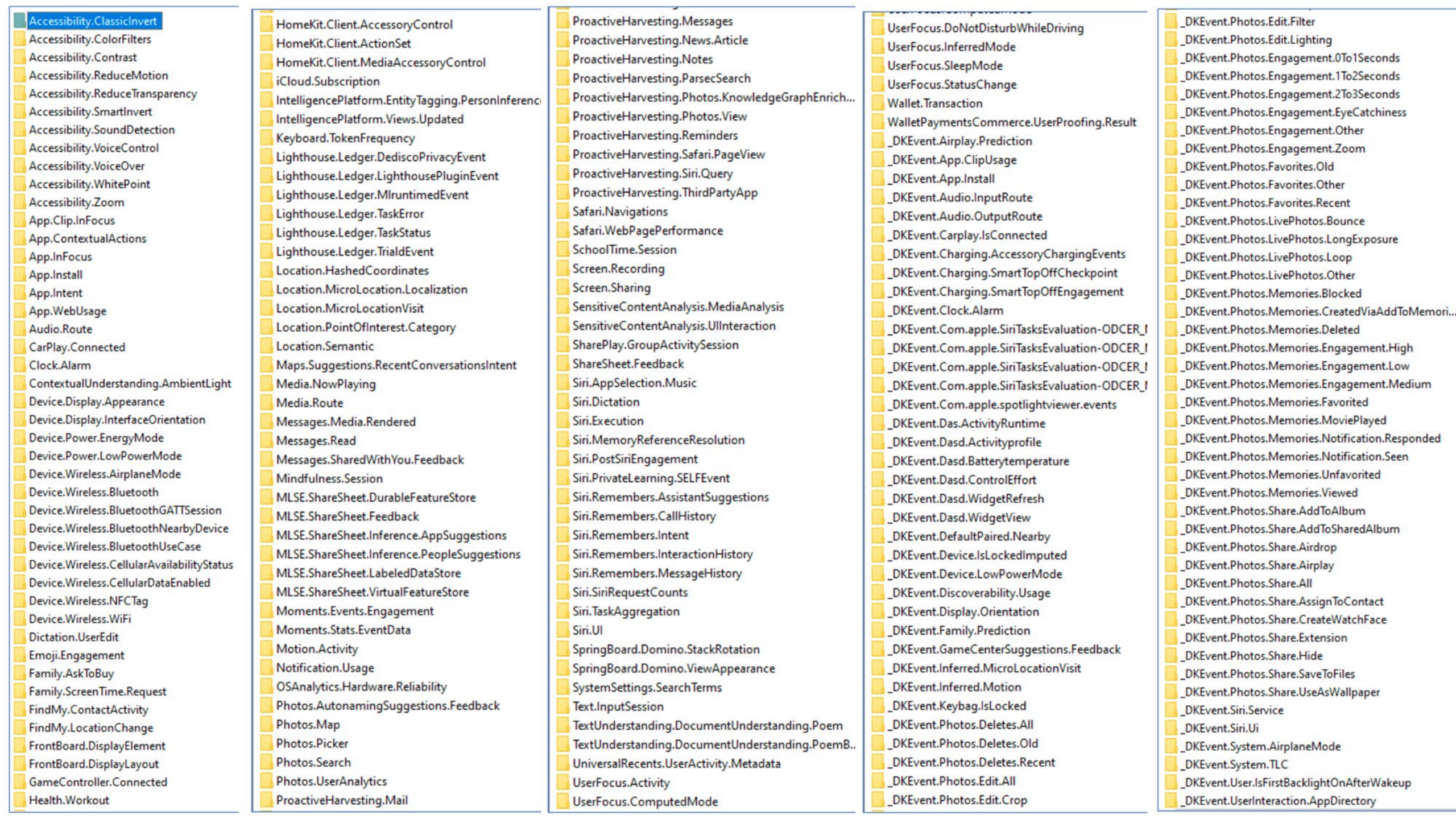

KnowledgeC
AirDrop 0 / 0 Records
Airplane Mode 0 / 0 Records
Application Focus 0 / 0 Records
App Intents - / 3924 Records
Application Usage - / 10162 Records
AudioRoute 0 / 0 Records
Backlight - / 8101 Records
Battery Temperature 0 / 0 Records
Bluetooth Connections - / 139 Records
Device Locked - / 3526 Records
Do Not Disturb 0 / 0 Records
Keybag Lock 0 / 0 Records
Media Playing - / 1754 Records
Notifications 5238 / 5238 Records
Orientation 0 / 0 Records
PinDrops 0 / 0 Records
Siri 0 / 0 Records
Web Usage - / 1342 Records
WiFi Connections 0 / 0 Records
Find

Icon	StartTime	EndTime	Activity	MetaData	ImagePreview	Source
	22/06/2023 10:51:07 (UTC)		Notification Received	Clear Method : IndirectClear		knowledgeC.db [ZOBJECT : 407659]
	22/06/2023 11:02:24 (UTC)		Notification Received	Clear Method : Receive Bundle : net.whatsapp.WhatsApp		knowledgeC.db [ZOBJECT : 407684]
	22/06/2023 11:02:24 (UTC)		Notification Received	Clear Method : DefaultAction		knowledgeC.db [ZOBJECT : 407687]
	22/06/2023 11:02:24 (UTC)		Notification Received	Clear Method : IndirectClear		knowledgeC.db [ZOBJECT : 407688]
	22/06/2023 11:16:28 (UTC)		Notification Received	Clear Method : Receive Bundle : com.microsoft.skype.teams		knowledgeC.db [ZOBJECT : 407748]
	22/06/2023 11:16:28 (UTC)		Notification Received	Clear Method : IndirectClear		knowledgeC.db [ZOBJECT : 407753]
	22/06/2023 11:16:31 (UTC)		Notification Received	Clear Method : Receive Bundle : com.microsoft.skype.teams		knowledgeC.db [ZOBJECT : 407749]
	22/06/2023 11:16:31 (UTC)		Notification Received	Clear Method : IndirectClear		knowledgeC.db [ZOBJECT : 407752]
	22/06/2023 11:17:34 (UTC)		Notification Received	Clear Method : Receive Bundle : com.microsoft.skype.teams		knowledgeC.db [ZOBJECT : 407763]
	22/06/2023 11:17:34 (UTC)		Notification Received	Clear Method : IndirectClear		knowledgeC.db [ZOBJECT : 407776]
	22/06/2023 11:18:06 (UTC)		Notification Received	Clear Method : Receive Bundle : com.microsoft.skype.teams		knowledgeC.db [ZOBJECT : 407767]
	22/06/2023 11:18:06 (UTC)		Notification Received	Clear Method : IndirectClear		knowledgeC.db [ZOBJECT : 407775]
	22/06/2023 11:18:10 (UTC)		Notification Received	Clear Method : Receive Bundle : com.microsoft.skype.teams		knowledgeC.db [ZOBJECT : 407768]
	22/06/2023 11:18:10 (UTC)		Notification Received	Clear Method : IndirectClear		knowledgeC.db [ZOBJECT : 407774]
	22/06/2023 11:18:14 (UTC)		Notification Received	Clear Method : Receive Bundle : com.microsoft.skype.teams		knowledgeC.db [ZOBJECT : 407769]
	22/06/2023 11:18:14 (UTC)		Notification Received	Clear Method : IndirectClear		knowledgeC.db [ZOBJECT : 407773]
	22/06/2023 11:39:46 (UTC)		Notification Received	Clear Method : Receive Bundle : com.microsoft.skype.teams		knowledgeC.db [ZOBJECT : 407842]
	22/06/2023 11:39:46 (UTC)		Notification Received	Clear Method : IndirectClear		knowledgeC.db [ZOBJECT : 407877]
	22/06/2023 11:40:05 (UTC)		Notification Received	Clear Method : Receive Bundle : com.microsoft.skype.teams		knowledgeC.db [ZOBJECT : 407866]
	22/06/2023 11:40:05 (UTC)		Notification Received	Clear Method : IndirectClear		knowledgeC.db [ZOBJECT : 407876]
	22/06/2023 11:40:20 (UTC)		Notification Received	Clear Method : Receive Bundle : com.microsoft.skype.teams		knowledgeC.db [ZOBJECT : 407870]
	22/06/2023 11:40:20 (UTC)		Notification Received	Clear Method : IndirectClear		knowledgeC.db [ZOBJECT : 407875]

Device and application usage



- **Biome**
- Retention is **28 days**
- The new knowledgeC.db, introduced in iOS 15
- **More than 200 activities on iOS 17 and iOS 18**


Accessibility.ClassicInvert
Accessibility.ColorFilters
Accessibility.Contrast
Accessibility.ReduceMotion
Accessibility.ReduceTransparency
Accessibility.SmartInvert
Accessibility.SoundDetection
Accessibility.VoiceControl
Accessibility.VoiceOver
Accessibility.WhitePoint
Accessibility.Zoom
App.Clip.InFocus
App.ContextualActions
App.InFocus
App.Install
App.Intent
App.WebUsage
Audio.Route
CarPlay.Connected
Clock.Alarm
ContextualUnderstanding.AmbientLight
Device.Display.Appearance
Device.Display.InterfaceOrientation
Device.Power.EnergyMode
Device.Power.LowPowerMode
Device.Wireless.AirplaneMode
Device.Wireless.Bluetooth
Device.Wireless.BluetoothGATTSession
Device.Wireless.BluetoothNearbyDevice
Device.Wireless.BluetoothUseCase
Device.Wireless.CellularAvailabilityStatus
Device.Wireless.CellularDataEnabled
Device.Wireless.NFCTag
Device.Wireless.WiFi
Dictation.UserEdit
Emoji.Engagement
Family.AskToBuy
Family.ScreenTime.Request
FindMy.ContactActivity
FindMy.LocationChange
FrontBoard.DisplayElement
FrontBoard.DisplayLayout
GameController.Connected
Health.Workout
HomeKit.Client.AccessoryControl
HomeKit.Client.ActionSet
HomeKit.Client.MediaAccessoryControl
iCloud.Subscription
IntelligencePlatform.EntityTagging.PersonInferenc
IntelligencePlatform.Views.Updated
Keyboard.TokenFrequency
Lighthouse.Ledger.DediscoPrivacyEvent
Lighthouse.Ledger.LighthousePluginEvent
Lighthouse.Ledger.MlruntimedEvent
Lighthouse.Ledger.TaskError
Lighthouse.Ledger.TaskStatus
Lighthouse.Ledger.TrialdEvent
Location.HashedCoordinates
Location.MicroLocation.Localization
Location.MicroLocationVisit
Location.PointOfInterest.Category
Location.Semantic
Maps.Suggestions.RecentConversationsIntent
Media.NowPlaying
Media.Route
Messages.Media.Rendered
Messages.Read
Messages.SharedWithYou.Feedback
Mindfulness.Session
MLSE.ShareSheet.DurableFeatureStore
MLSE.ShareSheet.Feedback
MLSE.ShareSheet.Inference.AppSuggestions
MLSE.ShareSheet.Inference.PeopleSuggestions
MLSE.ShareSheet.LabeledDataStore
MLSE.ShareSheet.VirtualFeatureStore
Moments.Events.Engagement
Moments.Stats.EventData
Motion.Activity
Notification.Usage
OSAnalytics.Hardware.Reliability
Photos.AutonamingSuggestions.Feedback
Photos.Map
Photos.Picker
Photos.Search
Photos.UserAnalytics
ProactiveHarvesting.Mail
ProactiveHarvesting.Messages
ProactiveHarvesting.News.Article
ProactiveHarvesting.Notes
ProactiveHarvesting.ParsecSearch
ProactiveHarvesting.Photos.KnowledgeGraphEnrich...
ProactiveHarvesting.Photos.View
ProactiveHarvesting.Reminders
ProactiveHarvesting.Safari.PageView
ProactiveHarvesting.Siri.Query
ProactiveHarvesting.ThirdPartyApp
Safari.Navigations
Safari.WebPagePerformance
SchoolTime.Session
Screen.Recording
Screen.Sharing
SensitiveContentAnalysis.MediaAnalysis
SensitiveContentAnalysis.UIInteraction
SharePlay.GroupActivitySession
ShareSheet.Feedback
Siri.AppSelection.Music
Siri.Dictation
Siri.Execution
Siri.MemoryReferenceResolution
Siri.PostSiriEngagement
Siri.PrivateLearning.SELFEvent
Siri.Remembers.AssistantSuggestions
Siri.Remembers.CallHistory
Siri.Remembers.Intent
Siri.Remembers.InteractionHistory
Siri.Remembers.MessageHistory
Siri.SiriRequestCounts
Siri.TaskAggregation
Siri.UI
SpringBoard.Domino.StackRotation
SpringBoard.Domino.ViewAppearance
SystemSettings.SearchTerms
Text.InputSession
TextUnderstanding.DocumentUnderstanding.Poem
TextUnderstanding.DocumentUnderstanding.PoemB...
UniversalRecents.UserActivity.Metadata
UserFocus.Activity
UserFocus.ComputedMode
UserFocus.DoNotDisturbWhileDriving
UserFocus.InferredMode
UserFocus.SleepMode
UserFocus.StatusChange
Wallet.Transaction
WalletPaymentsCommerce.UserProofing.Result
_DKEvent.Airplay.Prediction
_DKEvent.App.ClipUsage
_DKEvent.App.Install
_DKEvent.Audio.InputRoute
_DKEvent.Audio.OutputRoute
_DKEvent.Carplay.IsConnected
_DKEvent.Charging.AccessoryChargingEvents
_DKEvent.Charging.SmartTopOffCheckpoint
_DKEvent.Charging.SmartTopOffEngagement
_DKEvent.Clock.Alarm
_DKEvent.Com.apple.SiriTasksEvaluation-ODCER_I
_DKEvent.Com.apple.SiriTasksEvaluation-ODCER_I
_DKEvent.Com.apple.SiriTasksEvaluation-ODCER_I
_DKEvent.Com.apple.SiriTasksEvaluation-ODCER_I
_DKEvent.Com.apple.spotlightviewer.events
_DKEvent.Das.ActivityRuntime
_DKEvent.Dasd.Activityprofile
_DKEvent.Dasd.Batterytemperature
_DKEvent.Dasd.ControlEffort
_DKEvent.Dasd.WidgetRefresh
_DKEvent.Dasd.WidgetView
_DKEvent.DefaultPaired.Nearby
_DKEvent.Device.IsLockedImputed
_DKEvent.Device.LowPowerMode
_DKEvent.Discoverability.Usage
_DKEvent.Display.Orientation
_DKEvent.Family.Prediction
_DKEvent.GameCenterSuggestions.Feedback
_DKEvent.Inferred.MicroLocationVisit
_DKEvent.Inferred.Motion
_DKEvent.Keybag.IsLocked
_DKEvent.Photos.Deletes.All
_DKEvent.Photos.Deletes.Old
_DKEvent.Photos.Deletes.Recent
_DKEvent.Photos.Edit.All
_DKEvent.Photos.Edit.Crop
_DKEvent.Photos.Edit.Filter
_DKEvent.Photos.Edit.Lighting
_DKEvent.Photos.Engagement.0To1Seconds
_DKEvent.Photos.Engagement.1To2Seconds
_DKEvent.Photos.Engagement.2To3Seconds
_DKEvent.Photos.Engagement.EyeCatchiness
_DKEvent.Photos.Engagement.Other
_DKEvent.Photos.Engagement.Zoom
_DKEvent.Photos.Favorites.Old
_DKEvent.Photos.Favorites.Other
_DKEvent.Photos.Favorites.Recent
_DKEvent.Photos.LivePhotos.Bounce
_DKEvent.Photos.LivePhotos.LongExposure
_DKEvent.Photos.LivePhotos.Loop
_DKEvent.Photos.LivePhotos.Other
_DKEvent.Photos.Memories.Blocked
_DKEvent.Photos.Memories.CreatedViaAddToMemori...
_DKEvent.Photos.Memories.Deleted
_DKEvent.Photos.Memories.Engagement.High
_DKEvent.Photos.Memories.Engagement.Low
_DKEvent.Photos.Memories.Engagement.Medium
_DKEvent.Photos.Memories.Favorited
_DKEvent.Photos.Memories.MoviePlayed
_DKEvent.Photos.Memories.Notification.Responded
_DKEvent.Photos.Memories.Notification.Seen
_DKEvent.Photos.Memories.Unfavorited
_DKEvent.Photos.Memories.Viewed
_DKEvent.Photos.Share.AddToAlbum
_DKEvent.Photos.Share.AddToSharedAlbum
_DKEvent.Photos.Share.Airdrop
_DKEvent.Photos.Share.Airplay
_DKEvent.Photos.Share.All
_DKEvent.Photos.Share.AssignToContact
_DKEvent.Photos.Share.CreateWatchFace
_DKEvent.Photos.Share.Extension
_DKEvent.Photos.Share.Hide
_DKEvent.Photos.Share.SaveToFiles
_DKEvent.Photos.Share.UseAsWallpaper
_DKEvent.Siri.Service
_DKEvent.Siri.Ui
_DKEvent.System.AirplaneMode
_DKEvent.System.TLC
_DKEvent.User.IsFirstBacklightOnAfterWakeup
_DKEvent.UserInteraction.AppDirectory

Biome Text Input Session

10_Monday_224424\data\private\var\mobile\Library\Biome\streams\public\TextInputSession\local

Show 15 entries Search:

SEGB Timestamp	Time Start	SEGB State	Bundle ID	Duration	Filename	Offset
2023-07-01 10:42:01.669105+00:00	2023-07-01 10:41:52.866593+00:00	Written	net.whatsapp.WhatsApp	8.759704947471619	706024085910491	594944
2023-07-01 11:02:58.988661+00:00	2023-07-01 11:02:56.249575+00:00	Written	net.whatsapp.WhatsApp	2.5555230379104614	706024085910491	595024
2023-07-01 11:03:00.714886+00:00	2023-07-01 11:02:58.847576+00:00	Written	com.apple.Spotlight	1.7817659378051758	706024085910491	595104
2023-07-01 11:03:07.131136+00:00	2023-07-01 11:03:04.843980+00:00	Written	com.facebook.Messenger	2.2559010982513428	706024085910491	595184
2023-07-01 11:04:11.149848+00:00	2023-07-01 11:03:10.391034+00:00	Written	com.facebook.Messenger	60.22119104862213	706024085910491	595264
2023-07-01 11:08:01.360934+00:00	2023-07-01 11:07:54.807271+00:00	Written	net.whatsapp.WhatsApp	6.546175956726074	706024085910491	595344
2023-07-01 11:09:27.972202+00:00	2023-07-01 11:09:27.906098+00:00	Written	org.whispersystems.signal	0.0547870397567749	706024085910491	595424
2023-07-01 11:11:11.527047+00:00	2023-07-01 11:09:28.171277+00:00	Written	org.whispersystems.signal	103.25682497024536	706024085910491	595504
2023-07-01 11:11:30.557049+00:00	2023-07-01 11:11:23.375034+00:00	Written	com.getdropbox.Dropbox	7.162280082702637	706024085910491	595584
2023-07-01 11:12:08.524715+00:00	2023-07-01 11:11:37.567245+00:00	Written	ph.telegra.Telegraph	30.838361024856567	706024085910491	595664
2023-07-01 11:14:11.952388+00:00	2023-07-01 11:12:34.096204+00:00	Written	com.apple.mobilemail	97.64822399616241	706024085910491	595744
2023-07-01 11:14:19.258978+00:00	2023-07-01 11:14:18.619201+00:00	Written	com.apple.mobilemail	0.6314491033554077	706024085910491	595824
2023-07-01 11:14:53.177723+00:00	2023-07-01 11:14:52.549731+00:00	Written	com.apple.mobilemail	0.6026209592819214	706024085910491	595904
2023-07-01 11:15:11.912571+00:00	2023-07-01 11:15:02.668562+00:00	Written	com.apple.mobilemail	9.200744986534119	706024085910491	595984
2023-07-01 12:15:47.344474+00:00	2023-07-01 12:15:46.481784+00:00	Written	com.apple.Spotlight	0.3347100019454956	706024085910491	596064

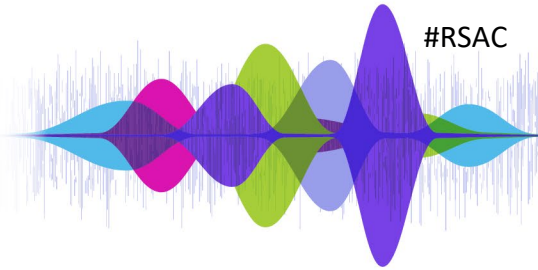
Wi-Fi Connections

10_Monday_224424\data\private\var\mobile\Library\Biome\streams\restricted\Device.Wireless.WiFi\local

Show 15 entries

Search:

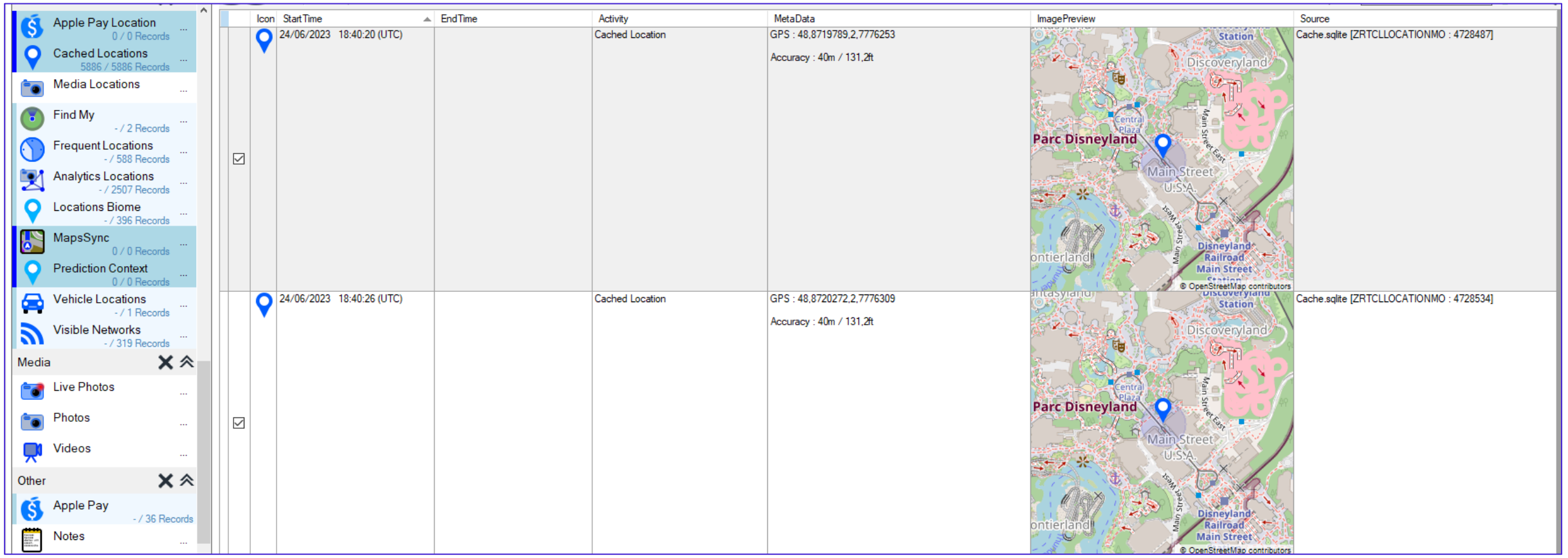
SEGB Timestamp	SEGB State	SSID	Status	Filename	Offset
2023-06-24 21:57:34.205622+00:00	Written	Sequoia-Lodge-Hotel	Connected	701866744756340	108864
2023-06-24 21:57:57.299565+00:00	Written	Sequoia-Lodge-Hotel	Disconnected	701866744756340	108920
2023-06-26 20:54:32.540416+00:00	Written	TIM-26153101	Connected	701866744756340	108976
2023-06-26 21:04:48.482009+00:00	Written	TIM-26153101	Disconnected	701866744756340	109024
2023-06-26 21:06:40.064740+00:00	Written	TIM-26153101	Connected	701866744756340	109072
2023-06-26 21:06:44.081531+00:00	Written	TIM-26153101	Disconnected	701866744756340	109120
2023-06-26 21:06:44.903088+00:00	Written	TIM-26153101	Connected	701866744756340	109168
2023-06-26 21:28:11.774361+00:00	Written	TIM-26153101	Disconnected	701866744756340	109216
2023-06-26 21:28:13.441324+00:00	Written	TIM-26153101	Connected	701866744756340	109264
2023-06-26 21:28:14.484175+00:00	Written	TIM-26153101	Disconnected	701866744756340	109312
2023-06-27 12:43:23.299283+00:00	Written	rnsys	Connected	701866744756340	109360
2023-06-27 12:43:29.415988+00:00	Written	rnsys	Disconnected	701866744756340	109408
2023-06-27 12:43:54.238502+00:00	Written	rnsys	Connected	701866744756340	109456
2023-06-27 17:30:43.976658+00:00	Written	rnsys	Disconnected	701866744756340	109504
2023-06-27 18:19:02.104624+00:00	Written	TIM-26153101	Connected	701866744756340	109552



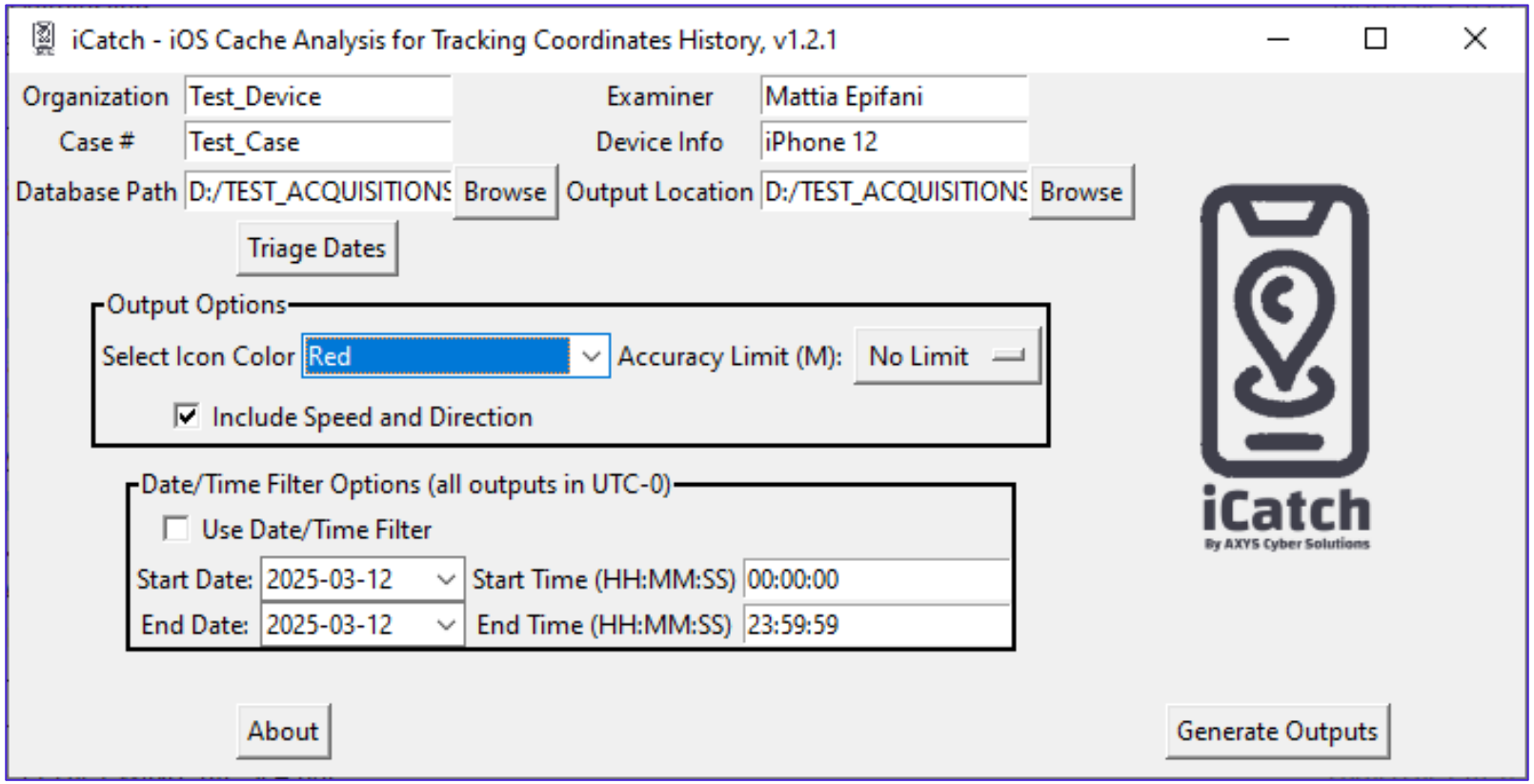
Geolocation

- **cache.sqlite**
- iOS Location Services Cache
- **All location requests lead to an entry in this database**
- Retention is **7 days**

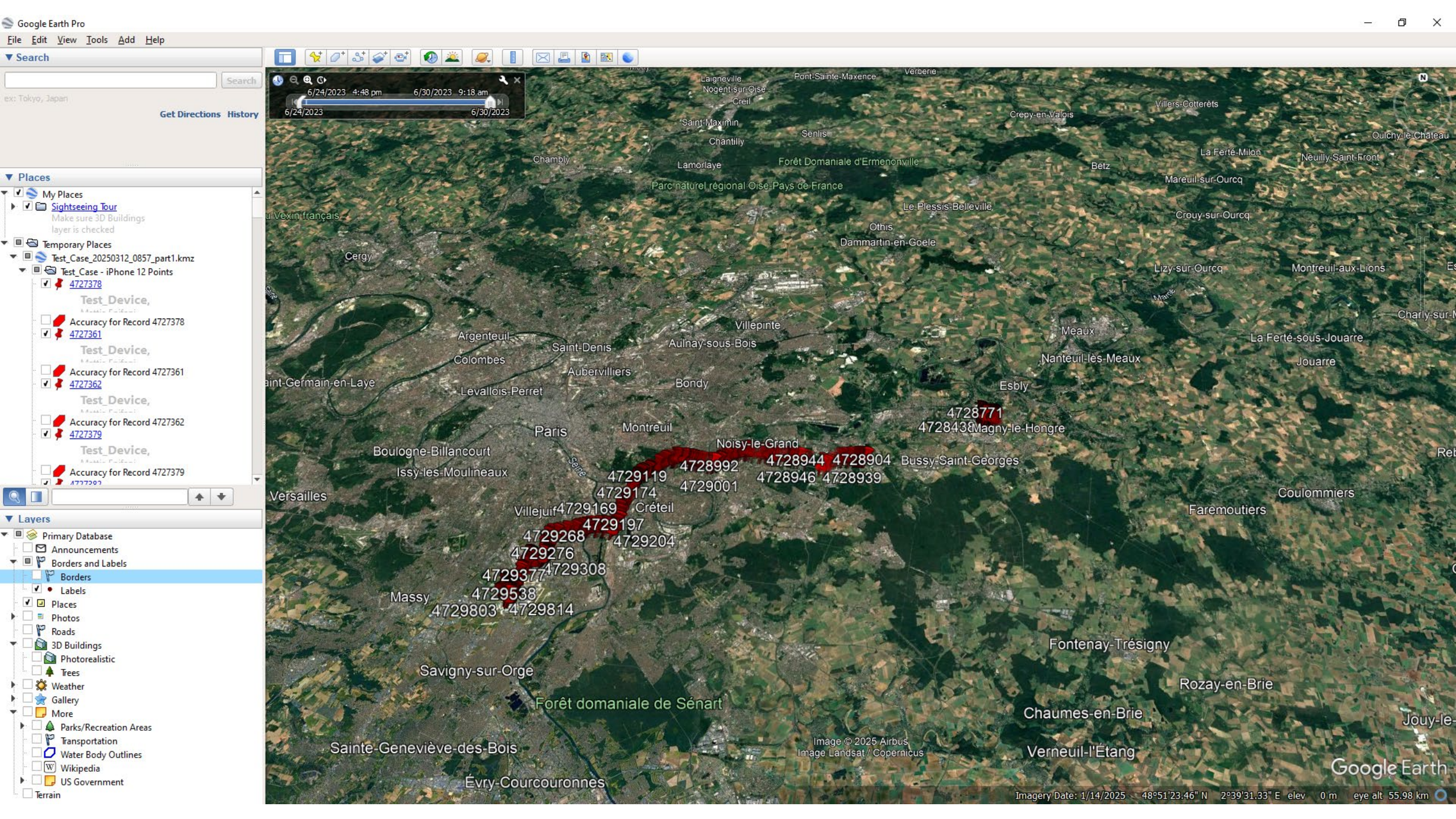
Cached Locations

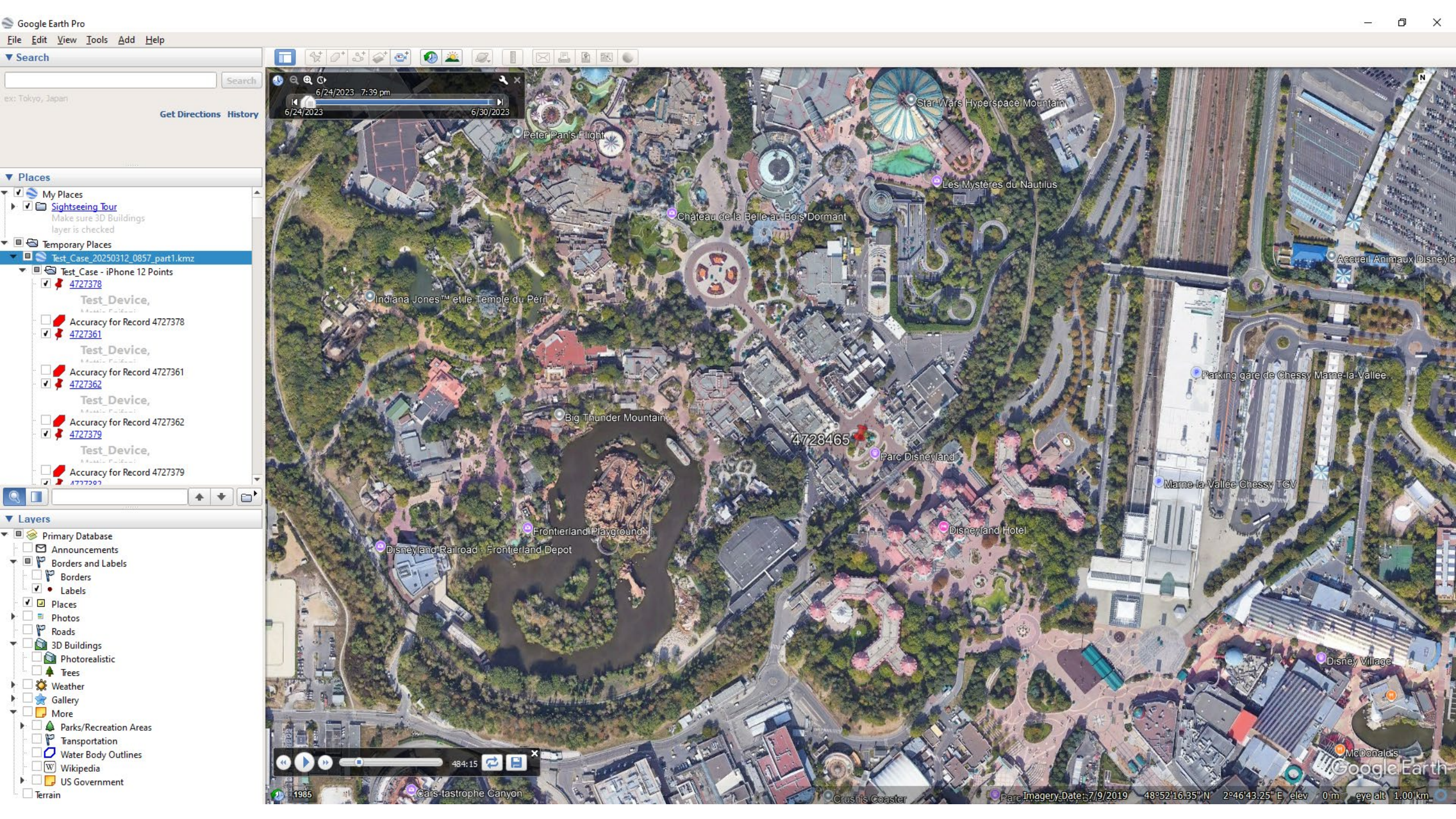


iCatch



https://github.com/AXYS-Cyber/iCatch

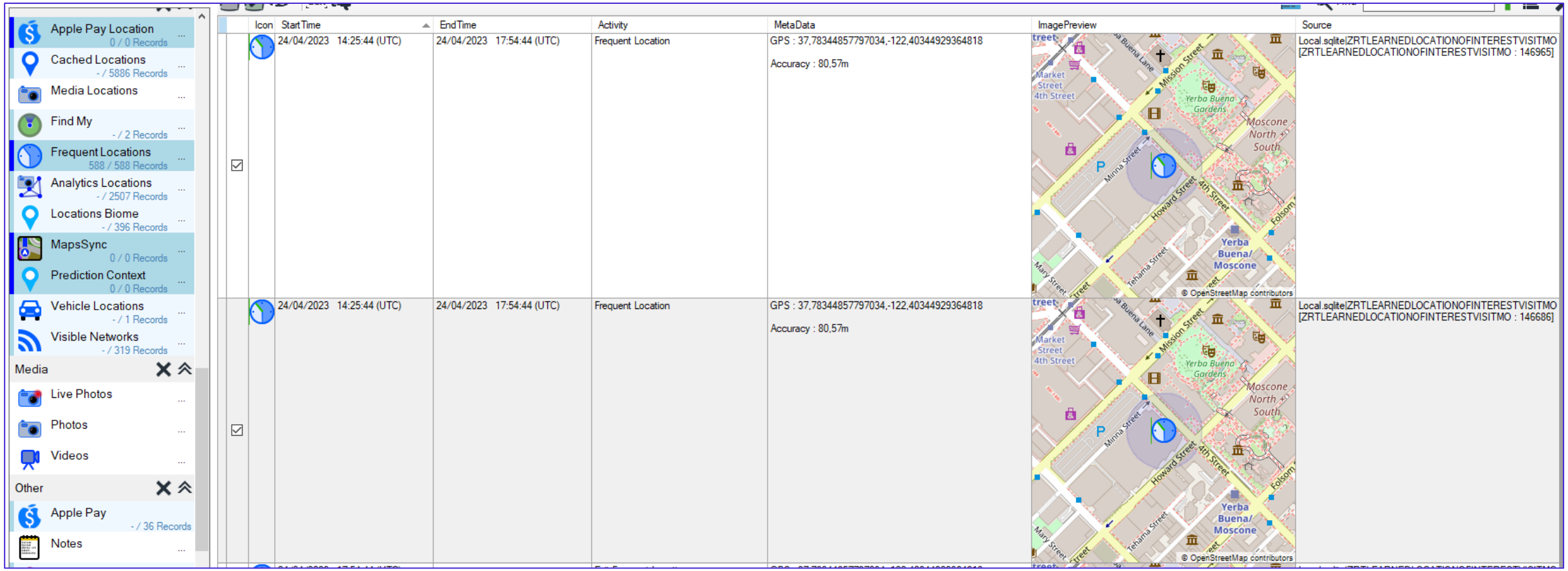

Google Earth Pro
File Edit View Tools Add Help
Search
Search
ex: Tokyo, Japan
Get Directions History
Places
My Places
Sightseeing Tour
Make sure 3D Buildings layer is checked
Temporary Places
Test_Case_20250312_0857_part1.kmz
Test_Case - iPhone 12 Points
4727378
Test_Device,
Accuracy for Record 4727378
4727361
Test_Device,
Accuracy for Record 4727361
4727362
Test_Device,
Accuracy for Record 4727362
4727379
Test_Device,
Accuracy for Record 4727379
Layers
Primary Database
Announcements
Borders and Labels
Borders
Labels
Places
Photos
Roads
3D Buildings
Photorealistic
Trees
Weather
Gallery
More
Parks/Recreation Areas
Transportation
Water Body Outlines
Wikipedia
US Government
Terrain
6/24/2023 4:48 pm
6/30/2023 9:18 am
6/24/2023
6/30/2023
Laigneville
Nogent-sur-Oise
Creil
Pont-Sainte-Maxence
Verberie
Villers-Cotterêts
Crépy-en-Valois
Saint-Maximin
Chantilly
Senlis
Oulchy-le-Château
La Ferté-Milon
Neuilly-Saint-Front
Chambly
Lamorlaye
Forêt Domaniale d'Ermenonville
Betz
Mareuil-sur-Ourcq
Parc naturel régional Oise-Pays de France
Le Plessis-Belleville
Crouy-sur-Ourcq
Othis
Dammartin-en-Goële
Cergy
Lizy-sur-Ourcq
Montreuil-aux-Lions
Villepinte
Argenteuil
Saint-Denis
Aulnay-sous-Bois
Meaux
La Ferté-sous-Jouarre
Colombes
Aubervilliers
Nanteuil-lès-Meaux
Jouarre
Bondy
Levallois-Perret
Esbly
4728771
4728438
Magny-le-Hongre
Paris
Montreuil
Noisy-le-Grand
Boulogne-Billancourt
Issy-les-Moulineaux
4729119
4728992
4728944
4728904
Bussy-Saint-Georges
4729174
4729001
4728946
4728939
Versailles
Villejuif
4729169
Créteil
Coulommiers
Faremoutiers
4729197
4729268
4729204
4729276
4729308
4729377
4729538
Massy
4729803
4729814
Fontenay-Trésigny
Savigny-sur-Orge
Rozay-en-Brie
Forêt domaniale de Sénart
Chaumes-en-Brie
Sainte-Geneviève-des-Bois
Verneuil-l'Étang
Évry-Courcouronnes
Image © 2025 Airbus
Image Landsat / Copernicus
Google Earth
Imagery Date: 1/14/2025 48°51'23.46" N 2°39'31.33" E elev 0 m eye alt 55.98 km


Google Earth Pro
File Edit View Tools Add Help
Search
Search
ex: Tokyo, Japan
Get Directions History
Places
My Places
Sightseeing Tour
Make sure 3D Buildings layer is checked
Temporary Places
Test_Case_20250312_0857_part1.kmz
Test_Case - iPhone 12 Points
4727378
Test_Device,
Accuracy for Record 4727378
4727361
Test_Device,
Accuracy for Record 4727361
4727362
Test_Device,
Accuracy for Record 4727362
4727379
Test_Device,
Accuracy for Record 4727379
Layers
Primary Database
Announcements
Borders and Labels
Borders
Labels
Places
Photos
Roads
3D Buildings
Photorealistic
Trees
Weather
Gallery
More
Parks/Recreation Areas
Transportation
Water Body Outlines
Wikipedia
US Government
Terrain
6/24/2023 7:39 pm
6/24/2023
6/30/2023
Star Wars Hyperspace Mountain
Peter Pan's Flight
Les Mystères du Nautilus
Château de la Belle au Bois Dormant
Accueil Animaux Disneyla
Indiana Jones™ et le Temple du Péril
Parking gare de Chessy Marne-la-Vallée...
Big Thunder Mountain
4728465
Parc Disneyland
Marne-la-Vallée Chessy TGV
Frontierland Playground
Disneyland Hotel
Disneyland Railroad - Frontierland Depot
Disney Village
484:15
1985
Cars-tastrophe Canyon
Crush's Coaster
McDonald's
Google Earth
Imagery Date: 7/9/2019 48°52'16.35" N 2°46'43.25" E elev 0 m eye alt 1.00 km

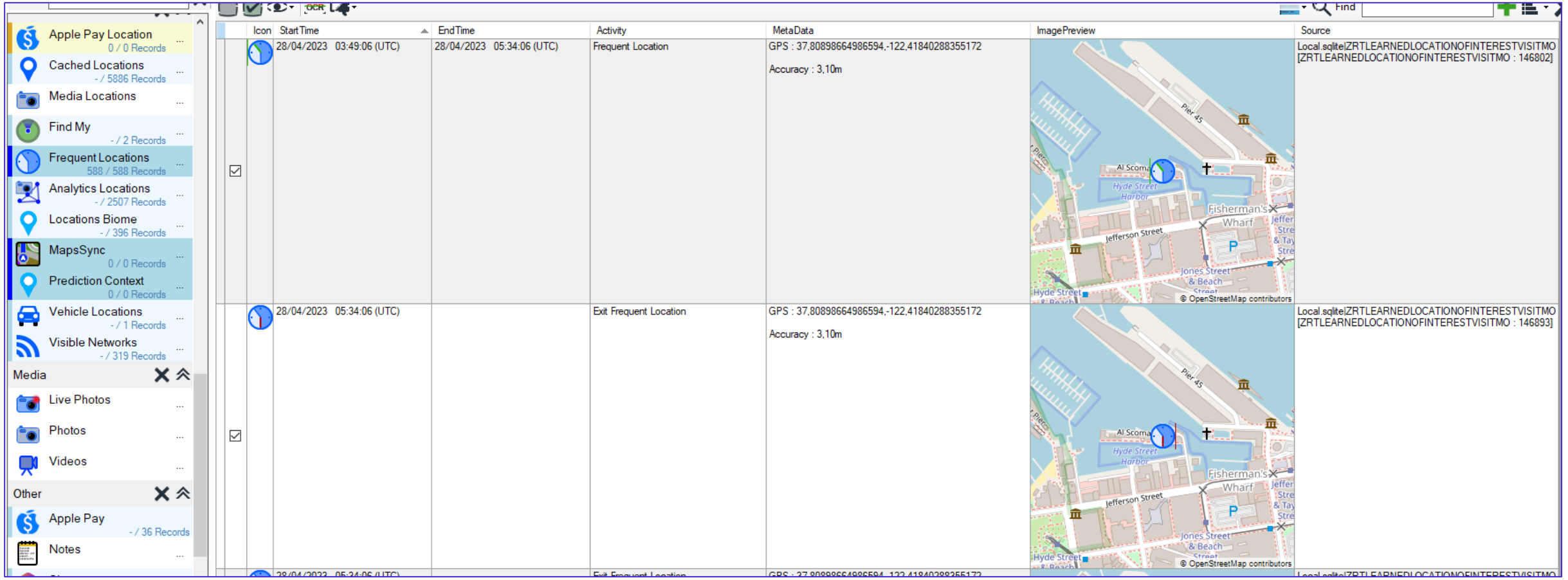
Geolocation

- **Local.sqlite / Cloud-V2.sqlite**
- **Significant/Frequent Locations**
- **Vehicle Locations**
- Retention is typically **90 days**

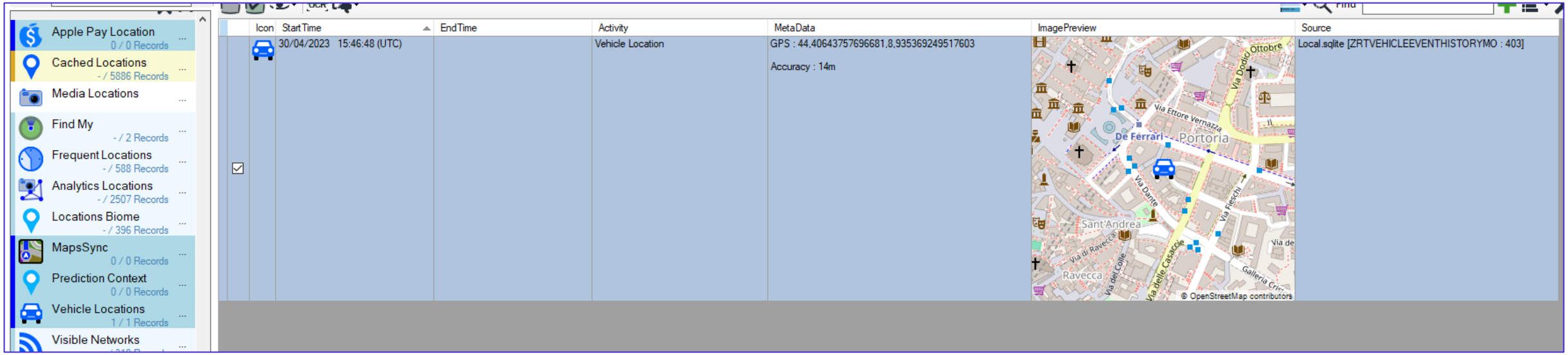
Frequent Locations (1)



Frequent Locations (2)



Vehicle Location



Health

- **healthdb_secure.sqlite**
- Unlimited retention
- Steps
- Heart rate
- Achievements
- Workouts
- Locations

Icon	StartTime	EndTime	Activity	MetaData
	09/04/2023 19:15:44 (UTC)	09/04/2023 19:16:45 (UTC)	Health Activity (Active Energy)	Active Energy : 1.2 Source : Apple Inc. Watch (Mattia's Apple Watch)
	09/04/2023 19:16:37 (UTC)	09/04/2023 19:17:31 (UTC)	Health Activity (Walking/Running Distance)	Walking/Running Distance : 31.88 m Source : Apple Inc. Watch (Mattia's Apple Watch)
	09/04/2023 19:16:37 (UTC)	09/04/2023 19:17:31 (UTC)	Health Activity (Steps)	Steps : 41 Source : Apple Inc. Watch (Mattia's Apple Watch)
	09/04/2023 19:16:42 (UTC)	09/04/2023 19:16:53 (UTC)	Health Activity (Step Length)	Step Length : 0.62 Source : Apple Inc. iPhone (IPhone12)
	09/04/2023 19:16:42 (UTC)	09/04/2023 19:16:53 (UTC)	Health Activity (Walking Speed)	Walking Speed : 0.77 Source : Apple Inc. iPhone (IPhone12)
	09/04/2023 19:16:45 (UTC)	09/04/2023 19:17:46 (UTC)	Health Activity (Active Energy)	Active Energy : 1.71 Source : Apple Inc. Watch (Mattia's Apple Watch)
	09/04/2023 19:17:12 (UTC)	09/04/2023 19:47:12 (UTC)	Health Activity (Environmental Sound Levels)	Environmental Sound Levels : 66.54 Source : Apple Inc. Watch (Mattia's Apple Watch)
	09/04/2023 19:17:46 (UTC)	09/04/2023 19:18:48 (UTC)	Health Activity (Active Energy)	Active Energy : 1.77 Source : Apple Inc. Watch (Mattia's Apple Watch)
	09/04/2023 19:18:32 (UTC)	09/04/2023 19:19:08 (UTC)	Health Activity (Walking/Running Distance)	Walking/Running Distance : 31.04 m Source : Apple Inc. Watch (Mattia's Apple Watch)
	09/04/2023 19:18:32 (UTC)	09/04/2023 19:19:08 (UTC)	Health Activity (Steps)	Steps : 44 Source : Apple Inc. Watch (Mattia's Apple Watch)
	09/04/2023 19:18:48 (UTC)	09/04/2023 19:19:49 (UTC)	Health Activity (Active Energy)	Active Energy : 1.58 Source : Apple Inc. Watch (Mattia's Apple Watch)
	09/04/2023 19:19:49 (UTC)	09/04/2023 19:20:09 (UTC)	Health Activity (Active Energy)	Active Energy : 0.4 Source : Apple Inc. Watch (Mattia's Apple Watch)

Passwords and Tokens

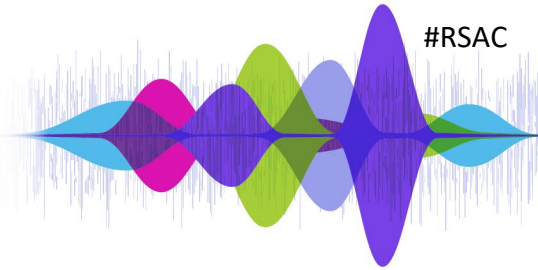
- **Keychain**
- Any app can store
  - Password
  - Encryption keys
  - Access tokens
- For example, Signal stores the encryption key for the local database in the Keychain

Account	Data	Label	Service
CcookiesDcastleR5 Guest	*SorryThereIsNoPasswordHere...	CcookiesDcastleR5 Guest	AirPort
DNCR-Aquarium_Visitor	NC@q2022	DNCR-Aquarium_Visitor	AirPort
FAIRHAVEN-5G	Fair9150	FAIRHAVEN-5G	AirPort
Gene_Frenkle	M0@r_c0WB3L1!!	Gene_Frenkle	AirPort
Happy Feet Planet_Guest	welcometotheplanet	Happy Feet Planet_Guest	AirPort
Matt_Foley	@V@n_D0wn_By_Th3_R1v3R!	Matt_Foley	AirPort
No_WiFi_For_You	@ComeBack1_Year!!	No_WiFi_For_You	AirPort
Stef0N	tH1s_PI@c3_haS_EverYtH1nG!!	Stef0N	AirPort
Techno24	Techno24	Techno24	AirPort
We're_Workin'_Here	*Whendidwegetmarried?*100...	We're_Workin'_Here	AirPort

RSAC 2025 Conference

Conclusions

Risks for users

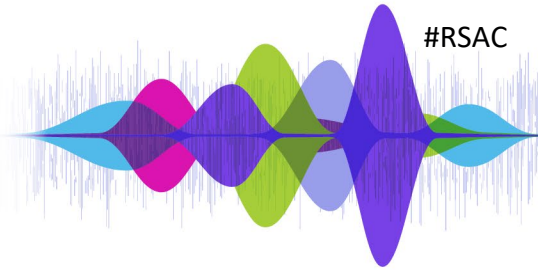


- A **stolen/lost device can expose a lot of information about yourself and/or your company**
  - Where you live
  - The places you've been
  - The applications you use
  - Your personal data (chats, multimedia, health)
  - Passwords and access tokens
- **Whatever you have done with your smartphone recently, it could still be on your smartphone and could be extracted!**

Apply: next week (act)

- On any personal device (smartphones/tablets)
  - Verify that you are **using a passcode**
    - Use long alphanumeric password to prevent brute force
  - Turn on **encrypted backups**
  - When not in use, **turn off location services**
  - **Clear applications cache regularly**
- On iOS devices
  - Disable control center access from lockscreen
  - Disable USB accessories
- On Android devices
  - Encrypt SD card, if in use

Apply: in the first three months (protect)

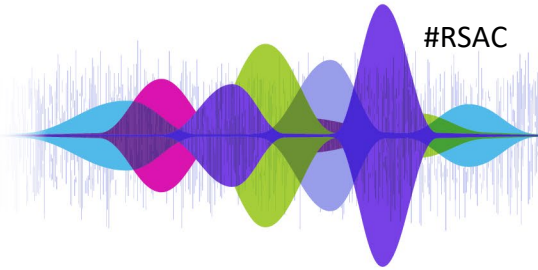


- Evaluate usage of advanced protection mechanisms
  - For Android devices, it depends on the manufacturer
  - For iOS devices
    - Turn off significant locations
    - Evaluate third party password manager instead of keychain
    - Stolen Device Protection
    - Advanced Data Protection for iCloud
    - Lock sensitive apps with Face ID
    - Lockdown Mode
- For enterprise devices:
  - Evaluate your MDM/MAM capabilities
  - Evaluate your EDR/Threat Protection capabilities

Apply: in the first three months (test)

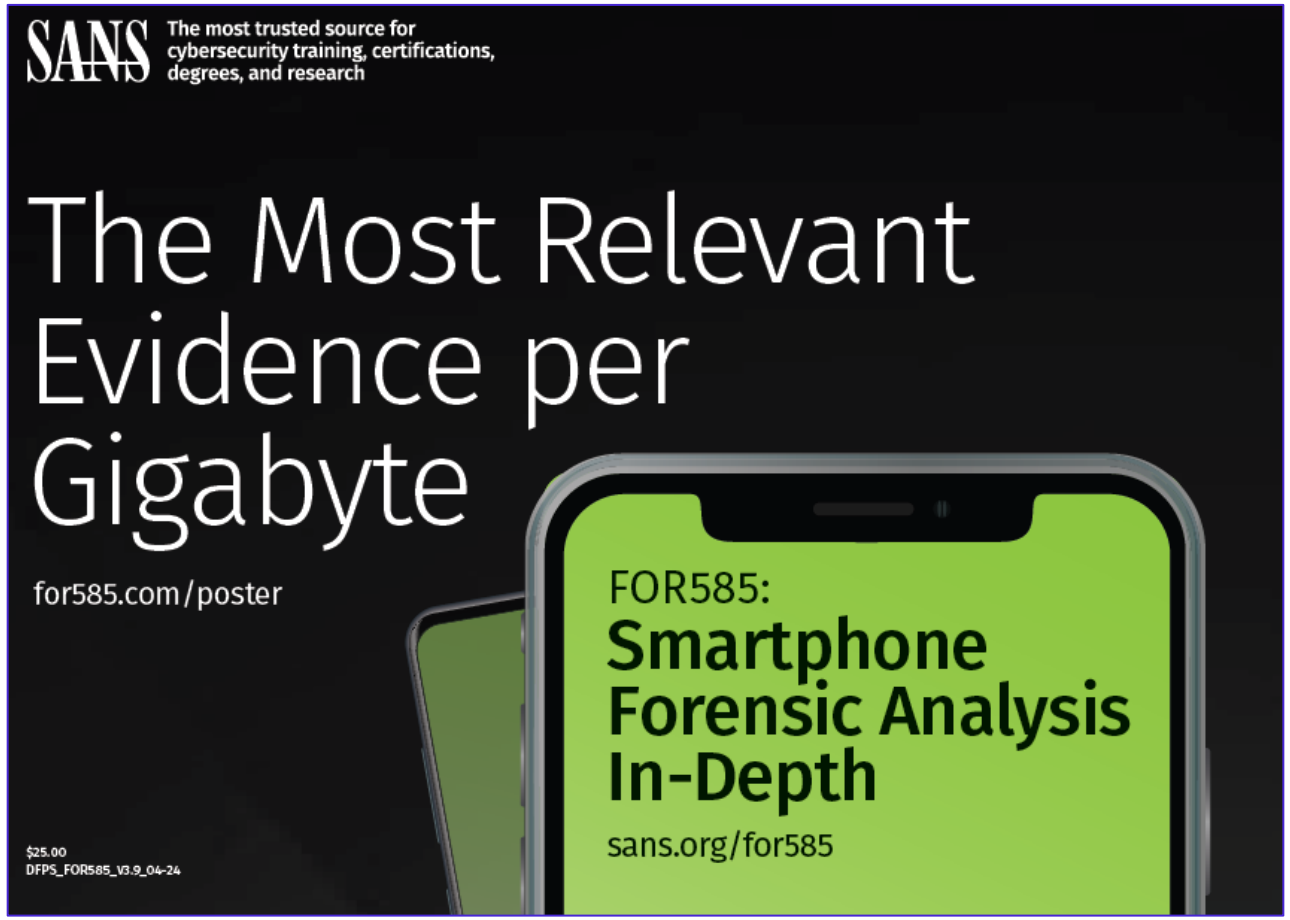
- Test what you have learned today with **test images**
- Various test images are freely available online
  - **Joshua Hickman Public Images**
    - https://thebinaryhick.blog/public_images/
    - Android 7 to Android 14
    - iOS 13 to iOS 17
  - **NIST CFReDS (Computer Forensic Reference DataSet)**
    - https://cfreds.nist.gov/
    - Cellebrite, Magnet and Belkasoft CTFs
    - Older phones/smarpthones

Apply: within six months (validate)



- Acquire your phone with free/opensource tools
  - **UFADE** for iOS
  - **Android Triage** and **Avilla Forensics** for Android
- Process the image with free/opensource tools
  - **iLEAPP** and **ArtEx** for iOS
  - **aLEAPP** and **Avilla Forensics** for Android
- For Business users: **perform regular risk assessments of test smartphones using advanced tools based on your MDM environment**
- Which information can you access?

The Most Relevant Evidence per Gigabyte



https://www.sans.org/posters/dfir-advanced-smartphone-forensics/

RSAC 2025 Conference

Many Voices.
One Community.

Mattia Epifani

mattia.epifani@realitynet.it